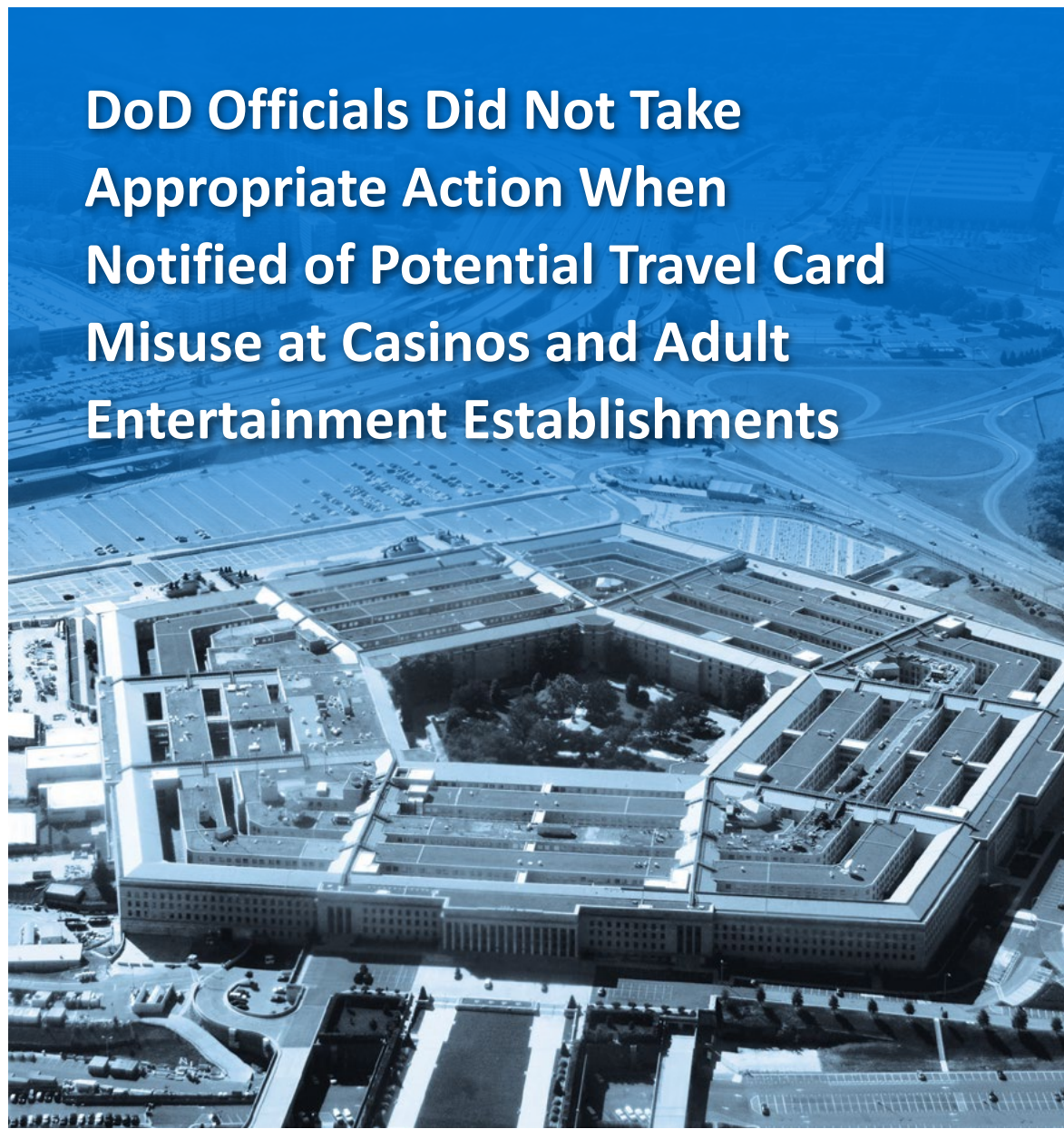




INSPECTOR GENERAL

U.S. Department of Defense

AUGUST 30, 2016



DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card Misuse at Casinos and Adult Entertainment Establishments

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.



Fraud, Waste, & Abuse

HOTLINE

Department of Defense

dodig.mil/hotline | 800.424.9098

For more information about whistleblower protection, please see the inside back cover.



Results in Brief

DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card Misuse at Casinos and Adult Entertainment Establishments

August 30, 2016

Objective

We determined whether DoD cardholders who used Government travel cards at casinos and adult entertainment establishments for personal use sought or received reimbursement for their charges. We also determined whether disciplinary action had been taken when personnel misused Government travel cards and if the misuse was reported to the appropriate security office.

This audit was a follow-up to a previous report we had issued, Report No. DODIG-2015-125, "DoD Cardholders Used Their Government Travel Cards for Personal Use at Casinos and Adult Entertainment Establishments," May 19, 2015. In response to that report, the Senate Committee on Armed Services requested an additional review. We performed this audit in response to that request.

Finding

We determined that DoD management (cardholder's commander or supervisor) and travel card officials did not take appropriate action when notified by the DoD OIG, during the previous audit, that cardholders had potentially misused their travel card. In this follow-up audit, we reviewed management's actions for 30 nonstatistically selected cardholders with the highest dollar amount of high-risk transactions that had been referred to management in the prior audit. During this audit, we found that:

- DoD management and travel card officials did not perform adequate reviews for the sampled cardholders;

Finding (cont'd)

- DoD management did not take action to eliminate additional misuse;
- DoD management did not initiate travel voucher reviews for cardholders with travel card personal use to determine whether there were improper payments; specifically, 22 of 29 cardholders (1 cardholder did not have travel vouchers during the period of review) sought and received reimbursements on 131 vouchers totaling \$8,544 that directly reimbursed or indirectly may have reimbursed the cardholder's personal use of the travel card (see Appendix D for DoD management collection efforts of overpayments); and
- DoD management did not consistently consider the security implications of improper personal use of the travel card; specifically, only 2 of 30 cardholders (5 cardholders did not have security clearances) were reported to the appropriate adjudicative facility prior to this audit (see Appendix E for DoD management actions on security clearances).

This occurred because Defense Travel Management Office officials and DoD management for the 30 selected cardholders did not emphasize proper use of the travel card, and DoD policy did not sufficiently specify what actions DoD officials should take when misuse was identified. As a result,

- the travel card program remained vulnerable to continued misuse;
- DoD had less money available for legitimate travel expenses because of the travel overpayments;
- DoD experienced potential national security vulnerabilities due to the untimely reporting or non-reporting of derogatory information regarding misuse of Government travel cards to the DoD Consolidated Adjudications Facility, resulting in the delay or lack of adjudication (decision on security clearance eligibility) for cleared DoD cardholders with financial concerns or personal conduct issues; and
- cardholders were not offered assistance for financial concerns and gambling addictions.

Visit us at www.dodig.mil



Results in Brief

DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card Misuse at Casinos and Adult Entertainment Establishments

Recommendations

We made several recommendations to address these problems. See the Recommendations section of the finding in the report. We recommend that the Under Secretary of Defense for Intelligence:

- report travel card misuse under investigation to the appropriate facility and the report outcome of the investigation; and
- report misuse of travel cards in a timely manner on individuals without a security clearance.

We recommend that the Director, Defense Travel Management Office, improve the identification of personal use of the travel card and disciplinary actions taken by revising the "Government Travel Charge Card Regulations."

Management Comments and Our Response

The Director, Counterintelligence and Security, responding for the Under Secretary of Defense for Intelligence, agreed with the recommendation, and addressed the specifics of the recommendation. Specifically, the Director stated the recommended requirements will be added to DoD 5200.02-R, which was converted to a manual and is expected to be published by December 31, 2016. Comments from the Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed with the recommendations but did not address the specifics of the recommendations on what actions that the Defense Travel Management Office would take to update the "Government Travel Charge Card Regulations." We request additional comments for these recommendations. Please see the Recommendations Table on the next page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Intelligence		1
Director, Defense Travel Management Office	2.a, 2.b, 2.d, 2.e, 2.f, 2.g.1, 2.g.3, and 2.i	2.c, 2.g.2, 2.g.4, and 2.h

Please provide Management Comments by September 30, 2016.





**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500**

August 30, 2016

**MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DIRECTOR, DEFENSE TRAVEL MANAGEMENT OFFICE**

**SUBJECT: DoD Officials Did Not Take Appropriate Action When Notified of Potential
Travel Card Misuse at Casinos and Adult Entertainment Establishments
(Report No. DODIG-2016-127)**

We are providing this report for review and comment. DoD management did not take appropriate action when notified that cardholders potentially misused their travel card at casinos and adult entertainment establishments. Specifically, DoD management and travel card officials did not perform adequate reviews for the cardholders reviewed and did not take action to eliminate additional misuse. Additionally, DoD management did not initiate travel voucher reviews for cardholders with travel card personal use to determine whether cardholders received improper overpayments and did not consistently consider the security implications of improper personal use of the travel card prior to this audit. We conducted this audit in accordance with generally accepted government auditing standards.

We considered management comments on a draft of this report when preparing the final report. DoD Instruction 7650.03 requires that recommendations be resolved promptly. Comments from the Director, Counterintelligence and Security, responding for the Under Secretary of Defense for Intelligence addressed the specifics of the recommendation, and no additional comments are required. Comments from the Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed with the recommendations but did not address the specifics of Recommendations 2.a, 2.b, 2.d, 2.e, 2.f, 2.g.1, 2.g.3, and 2.i. We request that the Director, Defense Travel Management Office provide additional comments that describe what actions have been taken or plan to take to accomplish the recommendations, and include the actual or planned completion dates of the actions by September 30, 2016.

Please send a PDF file containing your comments to aud-colu@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We cannot accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8901.

A handwritten signature in black ink, appearing to read "B. Baker", with a stylized, flowing script.

Dr. Brett M. Baker
Deputy Inspector General for Audit

Contents

Introduction

Objective	1
Prior Travel Card Audit Report	1
Sample Selection for this Audit	2
Travel Card Use	2
Improper Travel Voucher Payments	4
Security Clearance	5
Review of Internal Controls	6

Finding. DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card Misuse at Casinos and Adult Entertainment Establishments

7

DoD Management and Travel Card Officials Did Not Complete Adequate Reviews When Notified of Misuse	8
DoD Management and Travel Card Officials Did Not Take Action to Eliminate Further Misuse	19
Authorizing Officials Did Not Identify and Collect Overpayments	28
DoD Management Did Not Consider Security Implications of Travel Card Misuse	36
DoD Management Did Not Help Cardholders With Possible Gambling Addictions or Financial Concerns in a Timely Manner	43
Conclusion	44
Management Comments on the Finding and Our Response	44
Recommendations, Management Comments, and Our Response	45

Appendixes

Appendix A. Scope and Methodology	52
Use of Computer-Processed Data	56
Use of Technical Assistance	58
Prior Coverage	58
Appendix B. Senate Committee on Armed Services Request	59
Appendix C. Travel Card Misuse and Management Actions	60
Appendix D. Travel Overpayments	64
Appendix E. Security Clearance Considerations	67

Contents (cont'd)

Management Comments

Office of the Under Secretary of Defense for Intelligence	69
Deputy Assistant Secretary for Military Personnel Policy	70

Glossary	75
----------------	----

Acronyms and Abbreviations	77
----------------------------------	----

Introduction

Objective

We determined whether DoD cardholders who used Government travel cards at casinos and adult entertainment establishments for personal use sought or received reimbursement for their charges. We also determined whether disciplinary action had been taken when personnel misused Government travel cards and if the misuse was reported to the appropriate security office. See Appendix A for the audit scope and methodology related to the audit objectives. We performed this audit in response to a request on May 27, 2015, from the Senate Committee on Armed Services to conduct an additional review of actions taken by DoD management.

Prior Travel Card Audit Report

Public law¹ requires the Inspector General of each executive agency with more than \$10 million in travel card spending to conduct periodic audits or reviews of travel card programs to analyze the risk of illegal, improper, or erroneous purchases and payments. The findings of such audits or reviews, with recommendations to prevent improper use of travel cards, must be reported to the Director of the Office of Management and Budget (OMB) and Congress.

We issued Report No. DODIG-2015-125, “DoD Cardholders Used Their Government Travel Cards for Personal Use at Casinos and Adult Entertainment Establishments,” May 19, 2015. This report found that from July 1, 2013, through June 30, 2014, DoD cardholders had 4,437 transactions totaling \$952,258, where they likely used their travel cards at casinos for personal use and had 900 transactions totaling \$96,576 at adult entertainment establishments. On May 27, 2015, we received a request from the Senate Committee on Armed Services to conduct an additional review to address reimbursement for potential improper charges, security considerations due to misuse, and restriction of disciplinary actions due to labor agreements. See Appendix B for a copy of the Senate Committee on Armed Services request letter.

¹ Public Law 112-194, “Government Charge Card Abuse Prevention Act of 2012,” October 5, 2012.

Sample Selection for this Audit

We nonstatistically selected 30 cardholders with the highest dollar amount of high-risk² transactions referred in our prior audit to answer the Senate Committee on Armed Services' questions. Specifically, we reviewed:

- 7 cardholders who were examples from the prior adult report:³
 - 3 with misuse at casinos,
 - 3 with misuse at adult entertainment establishments, and
 - 1 with misuse at both casinos and adult entertainment establishments;
- 4 cardholders who used their travel card at adult entertainment establishments to cover all cardholders with adult entertainment use totaling \$1,000 or more; and
- 19 cardholders who used their travel card at casino automated teller machines (ATMs) or for quasi-cash transactions⁴ with the highest total dollar amount of referred potential personal use at casinos from the prior audit.

This report contains detailed examples for 13 of the 30 cardholders reviewed, and 3 of those 13 are repeated in more than one section. Appendix C, D, and E provide detailed information on the personal use totals and disciplinary actions taken, improper overpayments, and security clearance considerations for each of the 30 cardholders reviewed.

Travel Card Use

According to the Defense Travel Management Office (DTMO) website, the DoD Travel Card program provides travelers an effective, convenient, and commercially available method to pay for expenses related to official travel. Government travel card use is mandatory for all DoD personnel and is intended for official travel expenses only.

² In the prior report DODIG-2015-125 we identified and defined high-risk transactions, specifically transactions at adult entertainment establishments and transactions at casinos that met specific tests indicating likely personal use. We used those transactions identified in the prior audit to select a sample for this audit.

³ The seven cardholders who were detailed in the first report are cardholders 1 through 7 in the tables and when used as an example in this report.

⁴ Quasi-cash transactions such as transactions at a casino cage for noncash items including gambling chips.

DoD Financial Management Regulation

The DoD Financial Management Regulation (DoD FMR)⁵ set the policy for travel card use until March 2016 when the travel card policy within the FMR was replaced by the DoD Travel Card Regulations. It stated that the travel card was only for official travel related purposes, and travel card use while not on travel orders or not related to official Government travel requirements was misuse. The DoD FMR required agency program coordinators (APCs) to monitor all accounts for proper use and report accounts with unauthorized transactions to DoD management⁶ for action. The DoD FMR also required DoD management to ensure that cardholders used the travel card only for official travel related expenses.

DoD FMR Guidance Was Replaced During This Audit

The DoD Travel Card Regulations listed below replaced the travel card policy within the DoD FMR section on travel card use in March 2016. Although the guidance changed during our audit, we referred to the new guidance throughout this report in an effort to reduce redundancies between guidance. Changes to the DoD Travel Card Regulations included updates to incorporate recommendations we made during our prior audit and significant modifications to the cardholder statement of understanding. We also used the new guidance to ensure the audit did not make recommendations to outdated guidance or recommendations on problems that have been overcome by the improvements in the updated guidance. We did not have any findings or hold DoD management, travel card officials, or cardholders accountable for requirements that did not exist in the prior guidance.

Travel Card Instruction

DoD Instruction 5154.31⁷ replaced the travel card policy within the DoD FMR in March 2016. It establishes policy, assigns responsibilities, and provides procedures to manage the DoD Travel Card Program. The Instruction states that willful misuse of an individually billed travel card may result in disciplinary actions prescribed by local commanders and supervisors in accordance with DoD Travel Card Regulations.

⁵ DoD 7000.14-R "Financial Management Regulation," Volume 9, Chapter 3 "Department of Defense Government Travel Charge Card (GTCC)."

⁶ In this report, we refer to the cardholder's commander or supervisor or both as DoD Management.

⁷ DoD Instruction 5154.31, Volume 4, "Commercial Travel Management: DoD Government Travel Charge Card (GTCC) Program," October 16, 2015.

DoD Travel Card Regulations

The DTMO “Government Travel Charge Card Regulations,” March 2016, referred to as DoD Travel Card Regulations for the remainder of this report, states that travel card policies are applicable to all DoD personnel. Commanders and supervisors at all levels are required to ensure compliance with the DoD Travel Card Regulations. It states that, in each case of improper, fraudulent, abusive, or negligent use of the travel card, the commander or supervisor must take appropriate corrective or disciplinary action. The DoD Travel Card Regulations define misuse, which includes use while not on travel orders, as use at establishments or for purposes that are inconsistent with the official business of DoD or its standards of conduct.

Improper Travel Voucher Payments

The Defense Travel System (DTS) enables DoD travelers to create travel orders, generate travel vouchers for payment, and receive a split reimbursement between their bank accounts and the travel card vendor. It is DoD policy that DTS is the single, online travel system used by the DoD.

Improper Payment Definition

OMB⁸ defines an improper payment as any payment that should not have been made or was made in an incorrect amount under statutory, contractual, administrative, or other legally applicable requirements. Incorrect amounts are overpayments or underpayments that are made to eligible recipients. In addition, when an agency’s review cannot determine whether a payment was proper as a result of insufficient or lack of documentation, this payment must also be considered an improper payment.

We limited our review of improper payments to overpayments for this audit because the Senate Committee on Armed Services requested that we find when reimbursement was sought or received for improper charges.

Travel Regulations

The Joint Travel Regulations (JTR)⁹ governs travel and transportation at Government expense and applies to all DoD travelers. The JTR covers types of travel, transportation methods, and reimbursable expenses specifically stating which expenses are reimbursable and which are not. If DoD makes travel payments that do not comply with JTR requirements or payments for incorrect amounts, those payments are improper payments.

⁸ OMB Circular No. A-123, Appendix C, “Requirements for Effective Estimation and Remediation of Improper Payments,” October 20, 2014.

⁹ The Per Diem, Travel and Transportation Allowance Committee “The Joint Travel Regulations, Uniformed Service Members and DoD Civilian Employees,” (Updated monthly).

Security Clearance

DoD Instruction 5200.02¹⁰ establishes personnel security policies and procedures. DoD policy¹¹ set the standards for personnel security determinations to ensure an individual's eligibility for a security clearance is clearly consistent with the interests of national security and based upon careful consideration of criteria, including personal conduct and financial issues. The policy specifies several factors potentially related to travel card misuse including:

- disregard or violation of regulations or practices;
- criminal or dishonest conduct;
- acts of omission or commission that indicate poor judgment;
- excessive indebtedness, recurring financial difficulties, or unexplained affluence; and
- knowing and willful falsification, concealment, misrepresentation, or omission.

According to this policy, if questionable behavior patterns develop or derogatory information is discovered that could have an adverse impact on an individual's clearance eligibility, the potentially derogatory information must be reported to the commander or security officer for a significance review. In addition, the commander must ensure that the appropriate Consolidated Adjudications Facility is informed of both the derogatory information and any actions taken as a result of the derogatory information.

Commanders and security officials use the Joint Personnel Adjudication System (JPAS) to report and document travel cardholder derogatory information for adjudicator decision making.

¹⁰ DoD Instruction 5200.02, "DoD Personnel Security Program (PSP)," September 9, 2014.

¹¹ DoD 5200.2-R, "Personnel Security Program," January 1987, as amended February 23, 1996.

Review of Internal Controls

DoD Instruction 5010.40¹² requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses where DoD did not have specific controls in place that detailed the actions DoD officials should take when travel card misuse is identified.

- DTMO did not:
 - establish specific requirements for management to conduct reviews after potential travel card misuse was identified;
 - establish requirements to place restrictions on travel card accounts for cardholders with prior misuse or monitor travel card activity of cardholders with prior misuse more closely; or
 - establish timeframes for amending travel vouchers when an improper payment was identified.
- The Office of the Under Secretary of Defense for Intelligence did not require reporting derogatory information on travel card misuse to the appropriate adjudicative facility using JPAS.

We will provide a copy of the report to the senior officials responsible for internal controls in the Office of the Under Secretary of Defense for Intelligence and DTMO.

¹² DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013.

Finding

DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card Misuse at Casinos and Adult Entertainment Establishments

DoD management¹³ and travel card officials did not take appropriate action when notified that cardholders potentially misused their travel card. We reviewed management's actions for 30 nonstatistically selected cardholders¹⁴ with the highest dollar amount of high-risk transactions referred in the prior audit and found that:

- DoD management and travel card officials did not perform adequate reviews for the sampled cardholders;
- DoD management and travel card officials did not take action to eliminate additional misuse;¹⁵
- DoD management did not initiate travel voucher reviews for cardholders with travel card personal use to determine whether cardholders received improper overpayments; specifically, 22 of 29 cardholders¹⁶ sought and received overpayments on 131 vouchers totaling \$8,544 that directly reimbursed or indirectly may have reimbursed the cardholder's travel card personal use; and
- DoD management did not consistently consider the security implications of improper personal use of the travel card; specifically, only 2 of 30 cardholders¹⁷ were reported to the appropriate adjudicative facility using JPAS prior to this audit.

This occurred because DTMO officials and DoD management for the 30 selected cardholders did not emphasize proper use of the travel card, and DoD policy did not sufficiently specify what actions DoD officials should take when misuse was identified. As a result,

- the travel card program remained vulnerable to continued misuse;
- DoD had less money available for legitimate travel expenses because of the travel overpayments;

¹³ DoD management is the cardholder's commander or supervisor.

¹⁴ We referred high-risk travel card transactions at casinos and adult entertainment establishments to the Military Services and Defense Agency CPMs for review during our prior audit.

¹⁵ Personal use of a DoD travel card is misuse, we use the terms interchangeably throughout this report.

¹⁶ Only 29 of the 30 cardholders reviewed had travel vouchers during the period of review. One cardholder did not have any travel vouchers during the scope of our review.

¹⁷ Of the cardholders in our sample, 5 did not have a security clearance.

- DoD experienced potential national security vulnerabilities due to the untimely reporting or non-reporting of derogatory information to the DoD Consolidated Adjudications Facility, resulting in the delay or lack of adjudication (decision on security clearance eligibility) for cleared DoD cardholders with financial concerns or personal conduct issues; and
- cardholders were not offered assistance for potential financial concerns and gambling addictions.

DoD Management and Travel Card Officials Did Not Complete Adequate Reviews When Notified of Misuse

DoD management, component program managers (CPMs), and APCs did not perform adequate reviews, and, in some cases, did not perform any review after we notified them that the cardholders potentially misused their travel card at casinos or adult entertainment establishments. Specifically:

- CPMs and APCs did not report misuse to DoD management;
- APCs did not review transaction history for additional misuse;
- CPMs and APCs did not attempt to locate cardholders with suspected misuse;
- DoD management did not perform reviews of cardholder misuse in a timely manner; and
- DoD management's misunderstanding of a labor agreement prevented them from holding a cardholder accountable.

This occurred because DTMO officials and DoD management for the 30 selected cardholders did not emphasize proper use of the travel card, and DoD policy did not sufficiently specify what actions DoD officials should take when misuse was identified. See Appendix C for details on the amount of personal use we identified for each of the 30 cardholders reviewed.

DoD Travel Card Officials Did Not Report Misuse to DoD Management

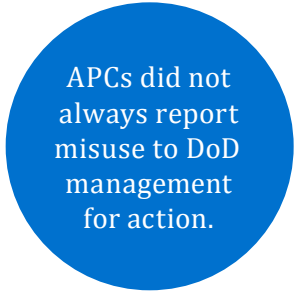
CPMs and APCs did not report travel card misuse to DoD management for appropriate action. During the prior audit, we referred casino and adult entertainment establishment transactions to the CPM for each Military Service and select Defense agencies.¹⁸

We asked the CPMs¹⁹ to review the transactions and determine whether they were personal use, whether the transactions had been previously identified, and whether actions have been or would be taken against the cardholder. In this audit, we determined that the CPMs had forwarded the transactions to APCs for review, but the APCs in some cases did not send the transactions to DoD management.

APCs are responsible to the commander/director at a lower level to execute and manage the day-to-day operations of the travel card program. In addition, APCs are required to monitor all accounts for proper use of the travel card and report accounts with unauthorized transactions to DoD management for action.

However, as shown in the example below APCs did not always report misuse to DoD management²⁰ for action. As a result, when misuse was not reported DoD management could not take action against cardholders for misuse, DoD management could not:

- initiate a review of the cardholder's transaction history to determine whether the cardholder had additional misuse,
- determine whether there were travel voucher overpayments, and
- report the incident in JPAS.



APCs did not always report misuse to DoD management for action.

We did not make a recommendation in this section because we make a recommendation in the “Improvements to Travel Card Trainings Could Enhance Travel Card Misuse Reviews” section of this report to revise APC training to include specific steps APCs should take when personal use, misuse, abuse, or fraud is found including who to contact.

¹⁸ We referred high-risk casino transactions to the Defense Contract Management Agency, the Defense Logistics Agency, and the Defense Threat Reduction Agency because they had five or more high-risk casino transactions.

¹⁹ A CPM establishes and maintains the travel card program at the component or agency level.

²⁰ DoD management monitors compliance with guidance and determines administrative or disciplinary actions for travel card misuse.

Army Lieutenant Colonel Misinformed APC, and APC Did Not Perform Her Responsibilities—Cardholder 25

During our prior audit, we identified an Army lieutenant colonel with potential travel card misuse. In December 2014, we referred 10 high-risk casino transactions totaling \$2,242 to the Army CPM. In February 2015, the cardholder acknowledged to the APC that his card use was inappropriate and stated:

I'm going to go ahead and let my commander know this investigation is occurring, provide him with the list of transactions in questions with my explanation of them, that way when the report comes out it's already old news to him. In conjunction with his JAG [Judge Advocate General] officer, who I'm certain will pour over all of the FMR [Financial Management Regulation], he will decide if my explanation is sufficient and what/if any action needs to be taken.

On November 17, 2015, we met with the cardholder's brigade commander, chief of staff, resource management officer, security manager, and command inspector general. They were not aware of the cardholder's personal use. The APC did not inform the cardholder's commander because the cardholder stated that he would notify his commander. The cardholder did not notify the commander nor did the APC follow-up to ensure the notification was made.

We informed the command about the 10 previously referred casino transactions totaling \$2,242 and 27 additional casino transactions totaling \$5,519 in our expanded review, as well as the cardholder's statement that he was going to inform his commander. As a result, the command deactivated the cardholder's travel card and did not allow the cardholder to travel. On the same day, the cardholder's access to classified information was suspended and the incident was referred to security clearance adjudicators using JPAS. On November 22, 2015, the commander initiated an investigation into the misuse with a suspense date of December 30, 2015. As of July 27, 2016, the investigation was complete, and the findings and recommendation were going through due process, which offers the cardholder an opportunity to comment before the commander issues disciplinary actions.

The APC's failure to notify the commander left him unaware of the original 10 casino transactions totaling \$2,242 that we referred in December 2014. The lack of notification also resulted in the commander's inability to investigate the cardholder's misuse and associated travel vouchers. If the commander was properly informed and able to investigate, he could have taken action on the original 10 transactions and initiated a travel card transaction history review, which would have identified the 27 additional casino transactions totaling \$5,519 and improper travel voucher payments where the traveler was not working but stayed at casinos and received meals and incidental expense payments. Finally, the commander could not report the incident in JPAS for nearly a year because he was unaware of the misuse.

The APC's failure to notify the commander left him unaware of the original 10 casino transactions totaling \$2,242 that we referred in December 2014.

APCs Did Not Review Transaction History for Additional Misuse

APCs did not review the cardholders' transaction history to identify additional misuse. The transactions we referred in the prior audit were selected based on 1 year of transaction history searched for specific key words, using data analysis tests, to identify the highest-risk transactions. It was not intended to be a stand-alone list of all potential personal use.

During this audit, we selected 30 cardholders identified in those transactions and reviewed the cardholder's travel card transaction history. For 22 of the 30 cardholders reviewed, cardholders had additional misuse outside of the transactions we referred or previously discussed with DoD management.

When APCs received the referred high-risk transactions, even in cases where they determined misuse occurred, the APCs did not look any further into the cardholders' transaction history. As a result, DoD management was not aware of the full scope of misuse and was unable to take appropriate action against the cardholders. As shown in the example below, the actions taken by DoD Management can be influenced by knowing the full scope of misuse.

The Director, DTMO should revise the "Government Travel Charge Card Regulations," March 2016, to require APCs to review the cardholder's transaction history to identify any additional travel card personal use, misuse, abuse, or fraud after misuse is suspected or referred for review.

Navy Civilian Abused Travel Card for Years, and the Extent of Misuse Went Undetected—Cardholder 22

During our prior audit, we identified a Navy civilian with potential travel card misuse. In December 2014, we referred 16 potential personal use transactions at casinos valued at \$2,439 to the Navy CPM. The referral provided multiple personal use indicators when referring the transactions to the Navy CPM, including:

- 12 of the 16 transactions occurred while the cardholder was not on orders; and
- 11 of the 16 transactions occurred at casinos on the same day as other potential casino misuse transactions.²¹

We met with the cardholder's first- and second-line supervisor, deputy comptroller, APC, human resource manager, and others. The APC shared that the cardholder was warned by the APC on several occasions dating back to 2007 about his ATM use. However, the Navy Consolidated Card Program Management Division still determined that none of the 16 casino transactions we referred were misuse.

The supervisors did not take action until we requested points of contact on August 27, 2015, to hold a meeting with command about the results of our prior audit. On August 27, 2015, the supervisor counseled the cardholder about his casino transactions. However, the supervisor and the APC still did not review the cardholder's transaction history for additional misuse.

Despite warnings dating to 2007, the casino transactions were not considered misuse initially and the APC did not review the cardholder for additional misuse.

The cardholder's transaction history showed an additional 258 misuse transactions totaling \$29,293 at casinos and card use while the cardholder was not on travel orders. Of those additional 258 transactions, 29 transactions totaling \$3,453 occurred after we notified the command of the potential personal use in December 2014. If the APC had reviewed the cardholder's transaction history, identified the additional misuse, and referred it to the supervisor, corrective or disciplinary action could have been taken to prevent the further misuse.

²¹ Some transactions met both indicators, so the sum of the bullets is more than the total number of transactions we referred.

We informed management of the travel card personal use and potential improper overpayments on travel vouchers on October 8, 2015. The cardholder's commander placed the cardholder on administrative leave beginning on November 6, 2015, while management was reviewing the cardholder's travel card use and travel vouchers. The commander also suspended the cardholder's access to classified information on November 10, 2015; however, on November 30, 2015, the cardholder retired before management's review was complete.

The Command Evaluation and Review Office completed its investigation on July 5, 2016. On August 5, 2016, the Commander approved 19 recommendations made in the investigative report.

Travel Card Officials Did Not Attempt to Locate Cardholders With Suspected Misuse

CPMs and APCs did not take steps to locate cardholders who had potential card misuse.

CPMs and APCs did not take steps to locate the cardholders who had potential card misuse after we referred the transactions to them. We asked the CPMs to review the transactions and determine whether they had been previously identified, whether they were personal use, and what actions or discipline has taken place for transactions found to be personal use.

CPMs reported inaccurate employment status for 4 of the 30 cardholders. Specifically, for two of the four cardholders, the CPMs reported that the cardholder was out of the Service; however, Citibank travel card accounts for the cardholders were still active in other commands. For the other two cardholders, the CPM reported that the command intended to counsel the cardholder, but the cardholders had retired before we referred the transactions in December 2014.

CPMs and APCs have access to multiple resources to locate a cardholder. These resources include, but are not limited to, the travel card bank system; the DoD travel systems; and personnel offices, which would have a record of whether the cardholder transferred or left the Service. As shown in the example below, the CPMs and APCs did not use the available resources to locate cardholders we referred for potential casino or adult entertainment establishment misuse. As a result, DoD management could not take action against cardholders who misused their travel card.

The Director, DTMO should revise the “Government Travel Charge Card Regulations,” March 2016, to require CPMs and APCs to verify the accurate employment status of a cardholder who has been identified or referred to DoD management for travel card personal use, misuse, abuse, or fraud.

*Army Captain Was Not Disciplined for Travel Card Misuse
Because the CPM and APC Did Not Take Basic Steps to Locate
the Cardholder—Cardholder 28*

During our prior audit, we identified a cardholder who was both an Army civilian and an Army Reserve captain with potential travel card misuse. In December 2014, we referred 14 casino transactions totaling \$2,014 to the Army CPM for review. On August 13, 2015, the Army CPM and APC reported that the transaction did not occur while the cardholder was on travel orders, meaning that the transactions were misuse; however, the CPM and APC reported that the cardholder separated from the Army and stated, “no action can be taken” against him. On September 25, 2015, the Army CPM provided the same response for the cardholder when he provided Army’s final response for its review of high-risk transactions.

On October 1, 2015, we reviewed the cardholder’s travel card account, to which the CPM and APCs also had access, and found that the card was still active and attached to a different Army organization, and we informed the CPM. On October 2, 2015, the Army CPM confirmed that the cardholder’s account was still active and coordinated to identify his current command. On October 15, 2015, the new Army organization confirmed that the cardholder was a current member of that command.

On November 4, 2015, we met with personnel from the cardholder’s previous command, current command, and Army Reserve Command Headquarters, including commanders, travel card officials, travel officials, and security. On November 18, 2015, the commander of the prior organization appointed an investigator to review the travel card use and make recommendations. On December 1, 2015, the investigator completed his investigation report and concluded that the cardholder

The CPM and APC reported the cardholder separated from the Army; however, we found the card was still active, and the cardholder was attached to a different Army organization.

misused his travel card and recommended a letter of reprimand. On March 23, 2016, the commander of the new organization provided the cardholder with the letter of reprimand for the travel card misuse.

Because the CPM and APC did not take steps to locate the cardholder, DoD management could not take action on the cardholder's 14 referred casino transactions totaling \$2,014 until we located the cardholder and notified his command. In addition, DoD management could not initiate a full review for additional misuse that could have identified an additional 18 transactions totaling \$2,388.

DoD Management Did Not Perform Reviews of Cardholder Misuse in a Timely Manner

After DoD management became aware of potential travel card misuse in our prior audit, it still did not take steps in a timely manner to review the cardholders' referred transactions and take appropriate action. The previous DoD FMR only required APCs to report cardholder misuse to the commander or supervisor. However, the DoD Travel Card Regulations also require DoD management to ensure that the travel card is used only for official travel related expenses and take action in cases of misuse. Additionally, DoD management is required to coordinate cardholder misuse with personnel from:

- legal;
- security, required only for military members; and
- human resources, required only for civilian cardholders.

The intent of the DoD Travel Card Regulations is to ensure that management emphasis is given to the importance of supervisors carefully considering all of the facts and circumstances in reaching a disposition that is warranted, appropriate, and fair and to emphasize personal accountability.

Reviews of travel card misuse were less effective when different functional areas were not represented. The establishment of a review team ensure that the commander or supervisor was aware of the full scope of the misuse, as well as any related improper overpayments, and could take appropriate corrective or disciplinary actions. Specifically, the following individuals or offices should be represented during a travel card misuse review.

- Commander or Supervisor—ensures proper use of the travel card, takes appropriate disciplinary or administrative action for misuse, initiates a travel voucher review, and ensures incidents are reported in JPAS;

- APC—identifies travel card misuse and has access to travel card transaction history;
- Travel Office—identifies when the cardholder was on official travel and reviews travel vouchers to determine whether the cardholder was reimbursed for the misuse;
- Comptroller—determines whether DoD funds have been affected and if the cardholder had access to other DoD resources that should be reviewed;
- Security—submits JPAS incident reports and provides input on whether a cardholder’s access to classified information should be suspended during the investigation;
- Legal—provides legal advice and would have input on whether anything found in the review was misuse or should be considered for criminal investigation; and
- Human Resources—provides advice on administrative or disciplinary actions and labor agreements for civilian personnel, as appropriate.

As shown in the example below, the establishment of a review team would allow the commander or supervisor to take appropriate corrective or disciplinary actions. We did not make a recommendation in this section because we make a recommendation in the “Improvements to Travel Card Trainings Could Enhance Travel Card Misuse Reviews” section of this report to develop a training course for DoD management on their responsibilities when potential travel card personal use, misuse, abuse, or fraud is detected to include detailed information on the steps DoD management should take and who to contact, including the commander or supervisor, APC, travel office, comptroller office, security office, legal office, and human resources office.

Air Force Lieutenant Colonel's Discipline for Misuse Was Not Finalized for Over a Year due to Command's Untimeliness—Cardholder 14

During our prior audit, we identified an Air Force Reserve lieutenant colonel with potential travel card misuse. In December 2014, we referred 23 high-risk casino transactions totaling \$4,152 to the Air Force CPM. DoD management did not perform a review of the misuse in a timely manner or identify all of the problems because not all relevant staff reviewed the cardholder in a timely manner, as shown in the timeline below.

- December 24, 2014: we referred the cardholder's 23 transactions to the Air Force CPM for review.
- July 8, 2015: the Air Force CPM reported that the command was consulting with the Judge Advocate General (JAG) on possible Uniform Code of Military Justice actions.
- August 18, 2015: we requested points of contact to hold a meeting.
- September 16, 2015: we followed up with those points of contact to inform them of our intent to hold a meeting with management and determine what actions were taken.
- September 18, 2015: the commander created a memorandum for record stating that:
 - on or about January 30, 2015, the cardholder was counseled; and
 - on or about August 15, 2015, a follow up counseling session occurred where the cardholder was told to take the travel card training, sign a travel card statement of understanding, warned about security clearance concerns with gambling, and encouraged to talk to a counselor for possible gambling addiction.²²
- September 18, 2015: the cardholder completed travel card training and signed a travel card statement of understanding.
- November 3, 2015: we met with the commander, comptroller, and APC to discuss the cardholder's 23 casino transactions totaling \$4,152 that were previously referred and 66 additional misuse transactions totaling \$10,219 from the cardholder's transaction history. The command had not consulted with the JAG.
- December 14, 2015: the comptroller completed the travel voucher review and confirmed overpayments.

²² The command did not provide documentation of either of these counseling sessions before the September 18, 2015, memorandum.

- January 8, 2016: the commander finally consulted with the JAG.
- January 10, 2016: the commander issued a letter of counseling.

The commander did not require the cardholder to complete travel card training and sign a new statement of understanding until 2 days after we notified the command that we planned to discuss the actions taken. Additionally, it took the commander over 1 year from our referral of casino transactions to actually consult with the JAG and issue a letter of counseling for a cardholder with 89 personal use transactions totaling \$14,371.

It took the commander over 1 year from our referral to issue a letter of counseling for a cardholder with 89 personal use transactions totaling \$14,371.

DoD Management's Misunderstanding of a Labor Agreement Prevented Management From Holding a Cardholder Accountable

DoD management was not restricted from taking disciplinary action against any of the seven cardholders in our sample who were employed under various labor agreements. However, in one case described below, DoD management could not take disciplinary action because the human resources supervisor misunderstood the agreement and did not take disciplinary action within 45 days of discovery of the travel card misuse as the labor agreement required. Once the misunderstanding was corrected, the 45-day standard had passed, and no disciplinary action was ever taken against the cardholder. We did not make a recommendation because this problem was a result of a misunderstanding and was not a systematic problem.

Air Force Civilian Was Not Disciplined Because Command Misinterpreted a Labor Agreement—Cardholder 3²³

An Air Force civilian was an example in our prior report. The cardholder was employed under a labor agreement and used his travel card for seven casino transactions totaling \$1,565. We referred these transactions to the command in September 2014. At that point, the human resources supervisor investigated the transactions, interviewed the cardholder, and determined that the transactions were misuse. The supervisor stated that the employee's labor agreement required management to investigate the misconduct within 45 days of the occurrence and no disciplinary action could be taken.

²³ This example on labor agreements was discussed as a specific example in our prior report.

However, the agreement required action within 45 days of the occurrence or management's awareness of the incident. Action could have been taken because the command was not aware of the casino misuse before our referral. We met with the cardholder's commander in August 2015, and she also stated that the opinion of the human resources supervisor was incorrect and disciplinary action could have taken place at the time. However, because that review and discussion took place in October 2014, the 45-day requirement impacted management's ability to take action now against the cardholder for travel card misuse at casinos, and no disciplinary action occurred.

DoD Management and Travel Card Officials Did Not Take Action to Eliminate Further Misuse

DoD management, CPMs, and APCs did not take action to eliminate further travel card misuse by cardholders with prior misuse. After determining that the cardholders misused their travel card at casinos and adult entertainment establishments:

- APCs did not monitor cardholders with prior misuse for continued travel card misuse;
- DoD management, CPMs, and APCs did not restrict travel card credit and cash advance limits for cardholders with prior misuse;
- DoD Management did not notify the new command of prior travel card misuse committed by the transferring cardholders; and
- APCs did not deactivate travel cards when cardholders left the Service.

DTMO improved travel card policy by issuing the new DoD Travel Card Regulations; however, improvements to travel card trainings could enhance travel card misuse reviews.

APCs Did Not Monitor Cardholders with Prior Misuse for Continued Misuse

APCs did not take appropriate action to eliminate additional travel card misuse by monitoring activity of cardholders with prior misuse. As a result of the transactions that we referred from our prior audit, DoD management confirmed misuse for 23 of the 30 cardholders in our current review. However, in response to the transactions referred during the prior audit, DoD management or travel card officials did not make a determination or determined transactions at casinos or adult entertainment establishments were not misuse for seven cardholders. DoD management now agrees that all 30 cardholders had travel card misuse.

We reviewed transaction histories to determine the extent of the cardholders' travel card misuse. We also reviewed recent transactions to determine whether the cardholder continued the misuse after DoD management and the APC were made aware. Of the 23 cardholders, 2 had additional misuse after DoD management disciplined the cardholders for prior misuse of the travel card. For both of these cardholders, DoD management was not aware of the continued misuse because the APC did not closely monitor these cardholders.

As shown in the example below, unless APCs continually monitor cardholders who have been disciplined for travel card misuse, DoD management could remain unaware of continued misuse.

The Director, DTMO should revise "Government Travel Charge Card Regulations," March 2016, to require APCs to monitor the activity of cardholders with prior misuse and report any additional travel card personal use, misuse, abuse, or fraud to commanders or supervisors immediately.

Defense Threat Reduction Agency Civilian Continued to Misuse Travel Card Despite Prior Discipline and Security Warning—Cardholder 20

During our prior audit, we identified a Defense Threat Reduction Agency (DTRA) civilian with potential travel card misuse. On January 13, 2015, we referred five potential travel card casino misuse transactions totaling \$2,523 to the DTRA CPM. In October 2015, the CPM gave us an April 2014 DTRA Inspector General's office report on the investigation of eight transactions, including three of the five that we referred. During the investigation, the cardholder stated that he thought personal use was acceptable as long as the bill was paid and that he did not believe he was ever trained on proper travel card use until March 2014. Regardless of the cardholder's statement, the DTRA Inspector General's report concluded that on at least eight occasions between June 2013 and February 2014, the cardholder misused his travel card in violation of DoD and DTRA policy.

On May 19, 2014, DTRA issued a letter of reprimand. DTRA also reported the misuse to the Defense Intelligence Central Adjudication Facility (DICAF). On June 29, 2015, DICAF issued an advisory letter related to the cardholder's travel card misuse and gambling activity, warning that further financial issues or poor judgment may result in a loss of clearance eligibility.

However we determined that despite the investigation, the letter of reprimand from DTRA, and the advisory letter from DICAF, the cardholder continued to misuse his travel card when his command activated it for travel. Specifically:

- misuse after the May 19, 2014, letter of reprimand from DTRA included:
 - September 11, 2014: ATM withdrawal of \$504.50 in Charles Town, West Virginia near a casino while he was not on travel orders.
 - January 8, 2015: ATM withdrawal of \$104.50 in Charles Town, West Virginia near a casino while he was on travel orders to a different location.
 - February 6, 2015: ATM withdrawal of \$304.50 in Charles Town, West Virginia near a casino while he was not on travel orders.
 - March 4, 2015: ATM withdrawal of \$144 at a casino in Black Hawk, Colorado, about 90 miles away from his temporary duty (TDY) location.
 - April 17, 2015: ATM withdrawal of \$504 at a casino in Black Hawk, Colorado, about 90 miles away from his TDY location.
- misuse after the June 29, 2015, advisory letter from DICAF included:
 - July 30, 2015: ATM withdrawal of \$204 at a casino in Black Hawk, Colorado, about 120 miles away from his TDY location.
 - September 20, 2015: ATM withdrawal of \$504 at a casino in Black Hawk, Colorado, about 120 miles away from his TDY location.

Despite the investigation, the reprimand, and the security warning, the cardholder continued to misuse his travel card.

From October 2010 through September 2015, the cardholder misused his travel card at casinos and ATMs totaling \$9,483. The misuse included five times after he was reprimanded by DTRA totaling \$1,562. Additionally, after the cardholder received that reprimand and an advisory letter from DICAF, he misused his card two more times totaling \$708.

The cardholder was allowed to maintain his access to classified information and continued to misuse his travel card for over a year after being disciplined by his command and in the months after being warned by the DICAF about the misuse. DTRA was not aware of the continued misuse of his travel card until we notified it because the APC did not closely monitor

the cardholder after he was identified as a cardholder with prior misuse. The DTRA Inspector General stated, “DTRA has one APC that monitors over 1,300 accounts. This accounts for many thousands of transactions being monitored by one person every month.”

On October 27, 2015, we notified DTRA of the continued misuse. DTRA then sent the new information to the DTRA Inspector General Office and DICAF. DTRA suspended the cardholder’s access to classified information on November 6, 2015; placed the cardholder on administrative leave on November 9, 2015; and indefinitely suspended the cardholder beginning on December 10, 2015, based on local classified information access suspension.

A final DICAF adjudication will be made upon completion of the ongoing DTRA Inspector General investigation. DTRA will wait until the DTRA Inspector General investigation is completed to take any final disciplinary or adverse action. As of August 3, 2016, the investigation was completed and awaiting a legal review.

DoD Management and Travel Card Officials Did Not Restrict Credit and Cash Advance Limits for Cardholders With Prior Misuse

DoD management, CPMs, and APCs did not restrict travel card limits after identifying cardholders with prior misuse and missed an opportunity to reduce or eliminate future misuse as required by the DoD Travel Card Regulations.

DoD Travel Card Regulations states that DoD management, through its APCs, may decrease the available cash limits based on mission needs, and that CPMs are also responsible for ensuring that reasonable credit limits are established and maintained. DoD management, CPMs, and APCs should take action to eliminate additional misuse by reducing or eliminating credit and cash advance limits for cardholders with prior misuse. However, the example below identifies a cardholder in our sample with cash advanced limits that were higher than the standard despite the identified travel card misuse.

The Director, DTMO should revise “Government Travel Charge Card Regulations,” March 2016, to require APCs, in conjunction with DoD management, and CPMs to consider reducing the credit limit and ATM limit for cardholders with prior misuse.

Air Force Lieutenant Colonel Was Given Higher Than Normal Cash Advance Limits Despite Years of Travel Card Misuse—Cardholder 14

During our prior audit, we identified an Air Force Reserve lieutenant colonel²⁴ with potential travel card misuse. In December 2014, we referred 23 potential misuse transactions at casinos totaling \$4,152 to the Air Force CPM. The cardholder had an additional 66 misuse transactions totaling \$10,219 in his transaction history. Based on the travel card misuse, the commander verbally counseled the cardholder, issued a letter of counseling to the cardholder, and encouraged the cardholder to talk to a counselor for a possible gambling addiction.

Although the command identified misuse and took corrective action in January 2015, the individual's travel card had a cash advance limit that was higher than standard. Specifically, in December 2015, the cardholder's travel card had a \$1,000 ATM limit, which was higher than the standard limit of \$665. DoD policy allows the commander to direct the APC to adjust the cardholder's travel card limits in Citibank's system.

The higher limit allowed the cardholder to make ATM withdraws totaling more than the standard travel card limit on at least four occasions. For example, the cardholder withdrew \$2,538 for a 21-day trip and \$1,946 for a 13-day trip. We notified the commander of the increased limit and, in coordination with the comptroller, the commander with the APC temporarily reduced the cash advance limit to the standard level of \$665. According to Citibank²⁵ information, the card is set to revert to a \$1,000 cash advance limit on January 2, 2017.

DoD Management Did Not Notify the New Command of Prior Travel Card Misuse Committed by the Transferring Cardholders

In some cases, DoD management was unaware that cardholders were previously identified and disciplined for travel card misuse and as a result could not implement appropriate safeguards to eliminate additional travel card misuse.

DoD management had several options to eliminate further travel card misuse, including deactivating the travel card when the cardholder was not in travel status, reducing or eliminating the card's ATM or purchase limit, or deciding not to issue a travel card to cardholders with prior misuse. However, we found that DoD management was not aware of prior travel card misuse even when cardholders had been previously disciplined.

²⁴ This cardholder was previously discussed in the "DoD Management Did Not Perform Reviews of Cardholder Misuse in a Timely Manner" section of this report.

²⁵ Citibank is the contracted provider for DoD travel cards.

As shown in the example below, the gaining activity (the cardholder's new command) was not aware of the cardholder's misuse of the travel card at prior commands. As a result, it could not put controls in place to prevent additional misuse.

The Director, DTMO should revise "Government Travel Charge Card Regulations," March 2016, to require the losing activity (cardholder's prior command) to notify the gaining activity of detected travel card personal use, misuse, abuse, or fraud for any transferring cardholders.

Air Force Civilian Misused Travel Card at Three Commands— Cardholder 19

During our prior audit we identified a former Air Force Reservist, currently an Air Force civilian, with potential travel card misuse. In December 2014, we referred eight casino ATM transactions totaling \$2,727 to the Air Force CPM. The cardholder's transaction history showed an additional 353 personal use transactions, totaling \$29,813.

As an Air Force reservist, the cardholder received a letter of reprimand based on travel card delinquency and misuse at the first command. However, no information about the cardholder's travel card delinquency or misuse was sent to his next assignment.

As a result, the new supervisor at the second command was not aware of prior travel card misuse and did not implement any additional controls to eliminate further misuse. While at the second command, the cardholder continued to use his travel card for personal use. Specifically, the cardholder had 225 transactions outside official travel totaling \$16,373 and 15 casino transactions totaling \$4,367. If the commander at the first command had notified the gaining DoD management of the travel card misuse, the supervisor or APC could have closely monitored the account and identified the personal use or put controls in place to prevent further misuse. DoD management did not detect the \$20,740 of misuse during the cardholder's time at the second command.

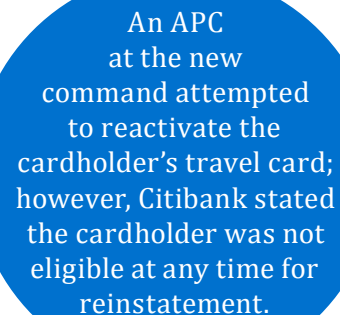
On May 4, 2014, the cardholder transferred to a civilian position at a third command, but, again, his supervisor and APC were unaware of his prior travel card misuse or letter of reprimand and could not implement additional controls to eliminate further misuse. In October 2014, the APC identified that the cardholder's travel card account was delinquent and

informed the supervisor. The APC's review of the cardholder's activity covered May 5, 2014, through September 4, 2015, and identified 136 personal use transactions for \$15,780, but the APC did not identify the personal use in the first and second commands. The supervisor stated that she attempted to call the cardholder's previous supervisors but did not receive a response.

The supervisor proposed a 14-day suspension and the commander sent the misuse to security, which temporarily suspended the cardholder's access to classified information. The cardholder responded to the suspension of his security clearance by stating that he was not properly trained and had severe financial difficulties, and he used the card to avoid "starving to death, becoming homeless, or being stranded in the desert due to no gas." The commander reduced the suspension to 7 days because "he [the cardholder] was in dire straits regarding finances and had no other options," and the commander did not believe there was any malicious intent behind his actions. In addition, the commander stated that this was the cardholder's first misconduct offense of any kind as a mitigating factor in his decision.

In November 2015, the cardholder accepted a civilian position at a fourth command and transferred on February 8, 2016. According to the cardholder's supervisor and APC at the fourth command, they were not informed of the prior misuse by the cardholder's previous command and the cardholder's personnel file was not provided to the new command.

On March 24, 2016, the cardholder's new APC at the fourth command attempted to reactivate the cardholder's travel card. However, Citibank denied the application and stated that the cardholder was not eligible at any time for reinstatement. The APC stated that the cardholder would use a centrally billed account to book airline tickets, would use personal credit cards for other travel expenses, and would not have personal access to the centrally billed account or account number.



An APC at the new command attempted to reactivate the cardholder's travel card; however, Citibank stated the cardholder was not eligible at any time for reinstatement.

The cardholder had 371 personal use transactions, including casino use, totaling \$35,332 at three different commands. The cardholder was disciplined for misuse twice, but his gaining commands were never notified of the travel card misuse or discipline. As a result, DoD management could

not implement appropriate safeguards. Additionally, the fourth command, unaware of the cardholder's history, attempted to reinstate his travel card, but Citibank denied the reinstatement eliminating this cardholder's potential for further abuse.

DoD APCs Did Not Collect or Deactivate Travel Cards When Cardholders Separated From the Service

The APCs did not deactivate travel cards after cardholders left Military Service. After cardholders separate or retire from the Service, they no longer perform official Government duties. As a result, they no longer need a travel card. DoD Travel Card Regulations state, "APCs will close a travel card account upon a cardholder's retirement, separation, termination or death..." and "...APCs will ensure/validate separated cardholder's accounts are properly closed."

As shown in the example below, if travel cards are not properly deactivated when the cardholder separates from the Service, misuse can continue.

The Director, DTMO should establish a working group with Citibank, CPMs, and others necessary to identify whether automated tools exist or could be developed to deactivate and close the travel card account automatically when cardholders separate.

Army Sergeant First Class Continued Travel Card Use After Separating From the Army—Cardholder 21

During our prior audit, we identified an Army National Guard first sergeant with potential travel card misuse. In December 2014, we referred 18 high-risk casino transactions totaling \$2,477 to the Army CPM. The Army CPM responded with the intent to counsel the cardholder. We contacted the cardholder's command, and it reported that the cardholder separated from the Army National Guard on May 31, 2014.

The cardholder used his travel card for automobile expenses, hotels, and casino ATMs for nearly 2 months after retirement. Specifically, the cardholder used his travel card 21 times totaling \$1,963 after separating from the Army. This occurred because the cardholder's APC stated that she was not aware of the cardholder's separation until November 2014, which was 6 months after the cardholder retired.

The cardholder used his travel card 21 times totaling \$1,963 after separating from the Army.

If the APC had been informed or an automated process to identify separating military members or civilians existed, the APC could have followed policy and closed the cardholder's travel card account when he separated from the Army, eliminating the potential for additional misuse.

Improvements to Travel Card Trainings Could Enhance Travel Card Misuse Reviews

DTMO has two courses²⁶ on travel card use; however, these courses have not been updated to comply with the DoD Travel Card Regulations. DTMO has an opportunity to improve training courses by incorporating travel card policy revisions into existing training programs. Training is a primary internal control to assure the proper use and monitoring of the travel card. Travel card training courses should be current, relevant, useful to the individual, and discuss management focus areas and observations on current trends. DTMO improved guidance for many aspects of the travel card program when it issued the DoD Travel Card Regulations. Specifically, the DoD Travel Card Regulations:

- clarified personal use and what the travel card can be used for;
- defined disciplinary actions and procedures, including coordination with security, legal, and human resources;
- required a mandatory review of the declined authorizations report, as recommended in our prior audit; and
- added that a statement of understanding on travel card use must now be re-certified and re-signed every 3 years.

Without training on the revised policy, cardholders, APCs, and supervisors risked misunderstanding their roles and responsibilities. The two courses on travel cards that DTMO has are:

- "Travel Card – Agency Program Coordinator" required initially and again every 3 years that describes the responsibilities of an APC; and
- "Travel Card 101" required initially and again every 3 years for all travel cardholders that describes the authorized uses of the travel card and responsibilities of cardholders.

²⁶ Refresher training may be obtained from other sources.

DTMO could improve the training courses by providing more examples of the types of misuse, abuse, and fraud that have been discovered. Additionally, the courses could explain the requirements for coordination in more detail as listed in the DoD Travel Card Regulations. DoD management would benefit from having a course developed that outlines their responsibilities for travel card misuse, including what steps should be involved in travel card misuse reviews and what the recommended disciplinary guidelines are for travel card misuse.

The Director, DTMO should revise the “Travel Card – Agency Program Coordinator” course to include examples of the types of travel card personal use, misuse, abuse, or fraud previously detected by DoD management.

The Director, DTMO the “Travel Card – Agency Program Coordinator” course to include detailed information on the steps APCs should take when travel card personal use, misuse, abuse, or fraud is found and who to contact including the commander or supervisor, travel office, comptroller office, security office, legal office, and human resources office.

The Director, DTMO should revise the Defense Travel Management Office “Travel Card 101” training course to include examples of the types of travel card personal use, misuse, abuse, or fraud previously detected by DoD management.

The Director, DTMO should develop a training course for DoD management on their responsibilities when potential travel card personal use, misuse, abuse, or fraud is detected to include detailed information on the steps DoD management should take and who to contact, including the commander or supervisor, APC, travel office, comptroller office, security office, legal office, and human resources office.

Authorizing Officials Did Not Identify and Collect Overpayments

DoD authorizing officials did not review travel vouchers for cardholders with travel card misuse to determine whether cardholders had been reimbursed for personal charges. Further, in response to our prior report, the Director, DTMO stated that personal use of the travel card did not result in the payment or loss of U.S. taxpayer dollars and cardholders must pay the cost of unauthorized or personal use transactions out of pocket. However, of the 29 cardholders who had travel vouchers, 22 sought and received improper reimbursements on 131 vouchers,

totaling \$8,544. The cardholders were directly reimbursed, indirectly may have been reimbursed, or both for their personal use of the travel card. Those improper overpayments included:

- lodging and meals for personal travel days;
- unsupported mileage reimbursements; and
- ATM fee reimbursement for misuse.

Additionally, although some improper payments were identified and confirmed, authorizing officials did not take action in a timely manner to recover identified overpayments. See Appendix D for details on the improper overpayments identified and length of time to collect.

Authorizing officials perform functions as a certifying officer when they approve DTS vouchers. They are required to check the accuracy of facts in a voucher and in supporting documents, verify compliance with the JTR, and determine the legality of the payment before they approve the voucher for payment.

If authorizing officials do not have sufficient information to determine whether a payment is correct, the payment should not be made. Once a payment is made, if the amount is incorrect or there is insufficient information to determine whether the amount is correct, it is an improper payment. Authorizing officials who perform certifying officer functions are financially liable for improper payments that result from improper certifications.

Authorizing Officials Did Not Identify Reimbursements for Unsupported Lodging and Meal Entitlements

Cardholders sought and authorizing officials approved reimbursement for lodging, meals and incidental expenses (M&IE), or both on days that were not associated with official travel or where supporting documentation showed that no expense was incurred.

DoD authorizing officials did not enforce the requirement for receipts or verify that these payments were for official travel as shown in the example below. Authorizing officials did not identify problematic vouchers because they did not follow up when lodging receipts showed irregularities.

The Director, DTMO should revise the “Government Travel Charge Card Regulations,” March 2016, to require DoD management and authorizing officials to compare travel vouchers to travel card activity to ensure lodging and M&IE charges are valid, accurate, and supported when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Air Force Technical Sergeant Made Misleading Statements and Authorizing Officials Did Not Identify Inconsistencies That Uncovered Falsified Information on a Voucher—Cardholder 26

An Air Force technical sergeant had a voucher that did not contain lodging receipts for all days that she was paid for M&IE. The traveler filed a voucher for a 7-day trip to Washington, D.C., stating that the travel was necessary to attend two training classes. The traveler claimed and was paid for 4 days of lodging and 7 days of M&IE.

We asked the command about the 2 days in which the traveler was not paid for lodging and why the voucher contained no hotel receipts for those days. The command informed us that the traveler stated that the room was “comp’d,” a word commonly associated with the casino providing a room free of charge to gamblers to encourage them to stay and gamble. In this case, the traveler stated that there was a problem with her hotel room, and the hotel in Alexandria, Virginia, gave her a free room for the final 2 nights. The travel voucher contained a hotel receipt showing that the traveler checked out prior to those 2 days. As a result, we questioned the accuracy of the information the traveler provided to her command and requested specific documentation on the problem at the hotel and confirmation of her training attendance.

Upon our request for evidence regarding the cardholder’s training attendance and accuracy of the statements made by the cardholder, the security manager investigated and found that the cardholder did not give any credible information for the training. The command personnel found one class scheduled on the 3rd and 4th day of her 7-day travel, but they could not find any evidence of the other class being offered during those dates.

The command contacted the hotel and found that there were no room problems, and the hotel did not provide a free room for the cardholder. The command identified toll charges showing that the traveler drove to Atlantic City, New Jersey on the 2nd day of her 7-day travel, but she returned to Washington, D.C. on the same day. They found that she went to Atlantic City on the 5th travel day and stayed there for the rest of the travel period.

As a result of the more thorough review of the cardholder's travel voucher, including an investigation of discrepancies between M&IE and hotel expenses and a review of the travel card transactions, the Commander determined the cardholder falsified information on an official travel voucher. The overpayments on the voucher totaled \$500.

The overpayment included 1 day of lodging when training did not exist and 3 days of M&IE when she was not performing any official duties. The commander also found that the cardholder was not in a leave status or in training or performing other DoD functions. The cardholder's supervisor charged the cardholder leave and established debts for the improper overpayments. The cardholder retired from the Air Force in March 2016 before she received discipline.

The cardholder falsified information on an official travel voucher and received overpayments totaling \$500.

Authorizing Officials Did Not Identify Reimbursements for False, Inflated, or Unallowable Mileage

Cardholders sought and authorizing officials approved reimbursement for personal vehicle mileage that was false, inflated, or unallowable. Authorizing officials could have used information from multiple sources to validate whether the traveler made a trip or not. One source of information is the travel card transaction history, which shows the location where transactions were made. If a transaction location does not correlate to the claimed location in a travel voucher, either the card has been compromised and is being used by another person, or the cardholder is not where they reported to be.

The Director, DTMO should revise the "Government Travel Charge Card Regulations," March 2016, to require DoD management and authorizing officials to review travel card transactions incurred by cardholders outside of official travel locations and other relevant sources of cardholder location to identify inflated or false mileage claims when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Local "in and around" mileage and mileage to transportation terminals such as airports or train stations are entered manually rather than using the Defense Table of Official Distances, which calculates reimbursable mileage based on required starting and ending points. According to the JTR, mileage that is manually entered, such as local "in and around" mileage, should be based on odometer readings. However, the number of miles driven is determined by the traveler and then submitted to the authorizing official for approval. The authorizing official should be required to review mileage claims closely, especially when travel card misuse has been identified or suspected.

The Director, DTMO should revise the “Government Travel Charge Card Regulations,” March 2016, to require DoD management and authorizing officials to review mileage that is manually entered and not based on the Defense Table of Official Distances to identify inflated mileage when travel card personal use, misuse, abuse, or fraud is identified or suspected.

The JTR states that mileage to and from dining locations during TDY is only allowed if meals are not available near the lodging or duty station and Government transportation is not available. As shown in the examples below, cardholders sought and received reimbursement for mileage that did not occur, inflated mileage, or unauthorized mileage.

The Director, DTMO should revise the “Government Travel Charge Card Regulations,” March 2016, to require DoD management and authorizing officials to review local mileage to identify mileage that is not reimbursable, including mileage claims for travel to restaurants or to perform personal errands when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Navy Civilian Filed False Vouchers, and the Authorizing Official Did Not Detect the Inaccuracies—Cardholder 22

A Navy civilian²⁷ filed claims on multiple vouchers for reimbursement of mileage that did not occur. We reviewed 2 years of vouchers from this cardholder and identified that in 9 of 36 vouchers, the cardholder claimed and was paid for mileage where travel card activity and other supporting documents showed that the traveler did not make at least part of those trips. The travel reported on the vouchers did not match the locations of the travel card use.

We reported those nine vouchers with false mileage claims to the cardholder’s command. The cardholder’s supervisor reviewed the nine vouchers and confirmed that the cardholder falsely filed travel claims for mileage. The supervisor determined that the traveler filed and was overpaid \$2,802 in false mileage claims for the 2-year period of our review. The cardholder also had the following additional improper overpayments:

- 27 of 36 vouchers reviewed were not appropriately limited to the authorized lower cost mode of transportation, as required by the JTR totaling \$2,408 in improper overpayments; and

The traveler filed and was overpaid \$2,802 in false mileage claims.

²⁷ Cardholder 22 was discussed previously in the “Navy Civilian Abused Travel Card for Years, and the Extent of Misuse Went Undetected” section of this report.

- 9 of the 36 vouchers reviewed had reimbursements for personal ATM fees, including casino use, totaling \$67 in improper overpayments.

After we informed DoD management of the travel card personal use and potential improper overpayments on travel vouchers, they reviewed the information we referred. The cardholder's commander placed the cardholder on administrative leave beginning on November 6, 2015, while management was reviewing the cardholder's travel vouchers. The commander also suspended the cardholder's access to classified information on November 10, 2015; however, on November 30, 2015, the cardholder retired before management's review was complete.

After our inquiries related to travel card misuse and other anomalies that we referred including timesheet irregularities, improper use of a Government vehicle, and falsified travel vouchers, Command Evaluation and Review Office personnel completed an investigation. On August 5, 2016, the Commander approved 19 recommendations made by the Review Office. The recommendations included actions to collect the overpayments identified for the cardholder, retraining of authorizing officials on limiting travel reimbursement to the authorized lower cost mode of transportation, and pecuniary liability of the certifying officer.

Army Civilian Filed Vouchers With Inflated Mileage, and the Authorizing Official Did Not Detect the Inaccuracies—Cardholder 16

An Army civilian who was also an Army Reserve staff sergeant had several vouchers with mileage that appeared excessive. The cardholder filed 4 of his 19 vouchers with mileage requests to and from the airport between 100 and 120 miles for each trip. However, the airport was 18 miles from the stated travel points; therefore the cardholder was entitled to 36 miles for each roundtrip to the airport. Additionally, because he was dropped off at the airport, a 36 mile roundtrip, and picked up from the airport, a 36 mile roundtrip, the total distance claimed should have been only 72 miles for each voucher.

The cardholder received \$85 in overpayments from these four vouchers with inflated mileage requests. The supervisor reviewed the vouchers, and agreed with our findings and amended the mileage to create debts for these improper overpayments in March 2016, on four travel vouchers, and the traveler repaid the debts in March 2016.

Army Lieutenant Colonel Filed Unauthorized Mileage Reimbursements, and the Authorizing Official Did Not Detect the Inaccuracies—Cardholder 8

An Army National Guard lieutenant colonel claimed and was paid for personal mileage, while on travel orders, on 3 of his 17 vouchers, totaling \$81, for travel to restaurants for breakfast, lunch, and dinner. The traveler did not indicate on the vouchers whether meals were unavailable near the duty station or lodging as required by the JTR for mileage reimbursement for travel to obtain meals. The vouchers also did not state if Government transportation was available as required by the JTR for mileage reimbursement for travel to obtain meals. On January 19, 2016, the cardholder amended all three vouchers to establish the debts and repaid the debts in February 2016.

Authorizing Officials Approved Reimbursement for Personal Use ATM Withdrawal Fees

DoD authorizing officials did not identify the overpayment of ATM fees associated with card misuse at casinos and adult entertainment establishments. While ATM fee reimbursements were allowed before FY 2015, reimbursement for misuse was never allowable. Specifically, the DoD Travel Card Regulations states, “ATM withdrawals during non-travel periods or not related to official Government travel requirements are ‘not authorized’ and are considered misuse.” Earlier guidance included that requirement and “any ATM fees charged by travel card vendor or ATM network operators for unauthorized withdrawals are NOT reimbursable.”

As noted above, ATM fee reimbursement ended on October 1, 2015; as a result, we are not making a recommendation to correct this problem. As shown in the example below, a cardholder sought and received reimbursement for ATM fees for a casino ATM withdrawal.

Air Force Civilian Sought and Received Direct Reimbursement for Casino Misuse—Cardholder 3

An Air Force civilian²⁸ claimed reimbursement for ATM fees related to his travel card misuse at casinos. A human resources supervisor reviewed the travel card transactions and determined that the casino transactions were for personal use during our first audit. However, the supervisor did not refer the voucher for review to determine whether the cardholder was directly reimbursed for those personal use transactions.

²⁸ This Air Force civilian was previously discussed in the “Air Force Civilian Was Not Disciplined Because Command Misinterpreted a Labor Agreement” section of this report.

The cardholder submitted and was directly reimbursed for ATM fees for misuse at casinos. In total, the traveler claimed and was improperly overpaid \$59 directly tied to casino misuse. A debt was created for the traveler in August 2015. On April 29, 2016, the cardholder submitted his reimbursement to the Defense Finance and Accounting Service.

The cardholder submitted and was directly reimbursed for ATM fees for misuse at casinos.

Authorizing Officials Did Not Recover Identified Overpayments in a Timely Manner

After we notified management of potential improper overpayments, authorizing officials did not take action to recover the identified overpayments in a timely manner. In the fastest collection from our audit, recovery of overpayments took DoD management 24 days: 15 days to amend the voucher and 9 days to collect the debt after the voucher was amended.

Travel voucher amendment initiates the collection actions for improper overpayments. In some cases the command has not amended the travel vouchers, or it took as many as 250 days after we notified the command for it to amend the voucher and initiate the debt collection. In addition, vouchers were amended and debts were established for several cardholders, but no collections have occurred as shown in the example below. As of August 8, 2016, some improper payments that we identified had not been collected.

DoD guidance²⁹ states that when travel voucher improper payments are identified, the voucher needs to be amended to create a debt. However, DoD guidance does not specify a timeframe for these corrections. DoD travelers are required to file vouchers within 5 days of the end of their travel. The same limitation should be required when amending vouchers to collect improper overpayments.

The Director, DTMO should revise the “Defense Travel System Regulations,” October 2015 to require travelers, authorizing officials, or non-DTS entry agents to amend travel vouchers within 5 days of identifying travel overpayments to establish a debt to recover the overpayment.

²⁹ DTMO “Guide for Managing Travel-Incurred Debt,” November 2, 2015.

Navy Civilian Retired Without Attempts to Collect Overpayments While Still in Service—Cardholder 22

A Navy civilian³⁰ had falsely claimed mileage and was paid \$2,802. The authorizing official confirmed that these payments were improper on November 2, 2015; however, no immediate action was taken to collect the improper overpayments. The cardholder retired on November 30, 2015, during the investigation into his travel card use and travel voucher claims.

As a result of this delay in collection and the cardholder's retirement, reimbursement from the traveler will not be efficient and will not include the option to transfer the debt to payroll offset within 30 days. The debt will transfer to the out-of-service debt process at the Defense Finance and Accounting Service, which will take additional resources and additional time to collect.

Despite the authorizing official's confirmation of falsely claimed payments on November 2, 2015, DTS does not show any collections actions taken regarding the improper payments for the cardholder as of August 8, 2016.

DoD Management Did Not Consider Security Implications of Travel Card Misuse

DoD management did not consistently take security implications of travel card misuse into consideration for 28 of the 30 cardholders reviewed. Specifically, only 2 of the 30 cardholders reviewed were reported in JPAS³¹ before we met with DoD management. As a result, DoD experienced potential national security vulnerabilities due to the untimely reporting or nonreporting of derogatory information to the DoD Consolidated Adjudications Facility. This resulted in the delay or lack of adjudication³² for cleared DoD cardholders with possible security concerns, including questionable judgment, unwillingness to follow rules and guidance, financial concerns, or gambling addictions.

³⁰ Cardholder 22 was previously discussed in the "Navy Civilian Filed False Vouchers, and the Authorizing Official Did Not Detect the Inaccuracies" section of this report.

³¹ JPAS is the master repository that provides the capability to perform comprehensive personnel security management of all DoD employees, military personnel, civilians, and DoD contractors.

³² The adjudicative process uses the whole-person concept where available, reliable information about the person, past and present, favorable and unfavorable, is considered.

The security clearance process involves an initial background investigation, periodic reinvestigations, and a process of continuous evaluation to ensure that individuals trusted with access to classified information are reliable, trustworthy, and able to protect classified information. Adjudicative Guidelines³³ state:

When a person's life history shows evidence of unreliability or untrustworthiness, questions arise whether the person can be relied on and trusted to exercise the responsibility necessary for working in a secure environment where protecting classified information is paramount.

Travel card misuse directly affects 2 of the 13 factors³⁴ considered when granting, revoking, or denying a security clearance:

- Personal conduct:
 - questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations; and
 - raises questions about an individual's reliability, trustworthiness, and ability to protect classified information.
- Financial considerations:
 - failure or inability to live within one's means, satisfy debts, and meet financial obligations;
 - problems related to gambling; and
 - behaviors that may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulation, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified information.

DoD 5200.2-R requires DoD management to inform the appropriate adjudicative facility of derogatory information and any actions taken or anticipated in response to that derogatory information in a timely manner. Reportable derogatory information are behaviors or information that could question an individual's trustworthiness, judgment, and reliability on the basis of the adjudicative guidelines, specifically personal conduct and financial considerations for travel card misuse.

Derogatory information is submitted to the adjudicators through JPAS. In JPAS there are initial, follow-up, and final incident reports. Derogatory information is reportable for all of the adjudicative guidelines and local security officers should file the initial incident report, follow up with remarks during the investigation,

³³ Adjudicative Guidelines determine eligibility for access to classified information.

³⁴ DoD 5200.2-R, Appendix 8, Adjudicative Guidelines for Determining Eligibility for Access to Classified Information.

and then finalized the report when the investigation is complete. DoD management has the option of suspending access to classified information before the final Consolidated Adjudications Facility adjudication. See Appendix E for details on the security considerations for each cardholder.

DoD Management Did Not Report Travel Card Misuse to JPAS



DoD management reported security incidents for only 2 of the 30 cardholders before this audit.

DoD management usually did not report derogatory information about travel card misuse using JPAS, although management agreed that misuse occurred for all of the cardholders reviewed. Specifically, DoD management reported security incidents for only 2 of the 30³⁵ cardholders before this audit. After meeting with us, security officers reported an additional ten cardholders, and one cardholder was reported for a second time for misuse between the prior report and this report.

DoD management did not refer the incidents for a variety of reasons. For example, management believed the person to be financially secure, the misuse was corrected, or the misuse was not a significant problem.

As shown in the example below, the Commander did not initially report the cardholder's travel card misuse to the appropriate adjudicative facility. As a result, the cardholder maintained access to classified information until the DoD Consolidated Adjudications Facility revoked the cardholder's classified information access and security clearance approximately a year after we referred the misuse.

The Director, DTMO should revise the "Government Travel Charge Card Regulations," March 2016, to require report of incidents of travel card personal use, misuse, abuse, or fraud under investigation or management review to the appropriate adjudicative facility in a timely manner using the appropriate personnel security system, and update with the final disciplinary action taken.

³⁵ DoD management or travel card officials originally determined only 23 of the 30 referred cardholders misused their travel cards at casinos or adult entertainment establishments.

Army Sergeant First Class Was Not Reported To Adjudicators for Nearly 1 Year—Cardholder 1

An Army Sergeant First Class was an example in our prior report. We notified the cardholder's command on September 19, 2014, about extensive travel card misuse at casinos and other ATMs while not on orders. The cardholder received a letter of reprimand on January 19, 2015, for 113 instances of travel card misuse. However, the cardholder was not reported to security at that time.

We met again with the cardholder's command during this audit on August 13, 2015, to discuss the actions taken and security considerations, and an incident was submitted to JPAS the same day. The following is the timeline of actions taken.

- September 17, 2015: the commander appointed an investigator to perform a 15-6 investigation to review travel card misuse and potential improper overpayments.
- January 27, 2016: the 15-6 investigation was completed.
- February 9, 2016: a general officer memorandum of reprimand was issued for the cardholder's travel card misuse.
- March 24, 2016: a second investigation was initiated because of higher-level command concerns about the scope and conclusions of the initial investigation.
- April 4, 2016: the second 15-6 investigation was completed and identified numerous problems including careless oversight of travel voucher reviews.
- April 19, 2016: the commander directed an audit of the cardholder's travel vouchers and recovery of any overpayments.
 - The audit identified eight travel vouchers totaling \$1,739.39 in overpayments; furthermore, the commander directed a third investigation including a review of additional travel vouchers.

On December 21, 2015, the DoD Consolidated Adjudications Facility made a preliminary decision to revoke the cardholder's classified information access and security clearance for personal conduct, financial considerations, and criminal conduct because it had not received an update on the initial incident report. As of August 5, 2016, the DoD

On December 21, 2015, the DoD Consolidated Adjudications Facility made a preliminary decision to revoke the cardholder's classified information access and security clearance.

Consolidated Adjudications Facility was continuing to perform a review of the cardholder's security clearance based on 15-6 investigative findings, including a finding that the cardholder chronically misused his travel card from January 2011 to November 2014.

Unreported Travel Card Misuse Incidents Had a Negative Impact on Security Clearance Adjudications

Security officials, including investigators and adjudicators, could not determine whether an applicant for a sensitive national security position was providing honest and trustworthy responses because DoD managers and commanders did not report travel card misuse to JPAS. DoD management's reporting of incidents in JPAS for travel card misuse is important because applicants for DoD security clearances must fill out the "Questionnaire for National Security Positions"³⁶ that specifically includes this question: "In the past seven (7) years have you been counseled, warned, or disciplined for violating the terms of agreement for a travel or credit card provided by your employer?"

The Under Secretary of Defense (Intelligence) should revise DoD 5200.2-R, "Personnel Security Program," to require commanders or supervisors, in coordination with security personnel, to report incidents of travel card misuse under investigation or management review to the appropriate adjudicative facility in a timely manner using the appropriate personnel security system.

The Under Secretary of Defense (Intelligence) should revise DoD 5200.2-R, "Personnel Security Program," to require commanders or supervisors, in coordination with security personnel, to report the outcome of the travel card misuse investigation including the results of the investigation and any administrative or disciplinary actions taken to the appropriate adjudicative facility using the appropriate personnel security system.

The Director, DTMO should revise the "Government Travel Charge Card Regulations," March 2016 to include in the commander's and supervisor's security reporting requirements travel card personal use, misuse, abuse, or fraud.

The Director, DTMO should develop a training course for DoD management on their responsibilities when potential travel card personal use, misuse, abuse, or fraud is detected, including security reporting requirements.

The following example describes an instance where a cardholder provided misleading information on the security questionnaire.

³⁶ Standard Form 86 "Questionnaire for National Security Positions," December 2010.

Navy Civilian Reported Misleading Information on National Security Questionnaire, and Adjudicators Were Unaware Because the Warnings Were Not Reported in JPAS—Cardholder 22

A Navy civilian³⁷ was not reported to the appropriate adjudicative facility using JPAS in a timely manner. The command provided documentation showing that the cardholder was warned at least five times in 2007 for misusing his travel card at casinos and while not on orders.

In January 2013, the individual underwent a periodic reinvestigation for his security clearance. The cardholder answered “no” to the to the Questionnaire for National Security Positions section that asked if in the last 7 years he was counseled, warned, or disciplined for violating the terms of agreement for a Government travel card.

Misuse of the travel card is a violation of policy and may impact security clearances, but misleading information on the SF 86 has additional importance and potential ramifications. On January 17, 2013, the cardholder signed his Questionnaire for National Security Positions certifying this statement:

My statements on this form, and on any attachments to it, are true, complete and correct to the best of my knowledge and belief and are made in good faith. I have carefully read the foregoing instructions to complete this form. I understand that a knowing and willful false statement on this form can be punished by the fine or imprisonment or both (18 U.S.C. 1001). I understand that intentionally withholding, misrepresenting, or falsifying information may have a negative effect on my security clearance, employment prospects, or job status, up to and including denial or revocation of my security clearance, or my removal and debarment from Federal service.

The cardholder’s command did not report the warnings or travel card misuse to the appropriate adjudicative facility using JPAS. As a result, the investigator and adjudicators were unaware of the withholding, misrepresentation, or falsification of the individual’s response during the individual’s security clearance review in 2013.

The investigator and adjudicators were unaware of the withholding, misrepresentation, or falsification of the individual’s response.

³⁷ Cardholder 22 was discussed previously in the “Navy Civilian Retired Without Attempts to Collect Overpayments While Still in Service” section of this report.

DoD Management Did Not Report Travel Card Misuse for Individuals Without a Security Clearance

DoD management did not report the travel card misuse to JPAS for any of the five cardholders without security clearances.

DoD management did not report the travel card misuse to JPAS for any of the five cardholders without security clearances.

DoD personnel with and without security clearances have JPAS profiles. Some individuals without a clearance are still subject to suitability determinations,³⁸ in some cases recurring periodically, and may be submitted for security clearance determination in the future.

DoD management should report travel card misuse in JPAS or other appropriate personnel security system to ensure adjudicators and suitability investigators have all relevant information about travel card misuse if and when they need to make a suitability or security clearance determination.

The Under Secretary of Defense (Intelligence) should revise DoD 5200.2-R “Personnel Security Program,” to require commanders or supervisors, in coordination with security personnel, to report incidents of travel card personal use, misuse, abuse, or fraud under investigation or management review to the appropriate adjudicative facility in a timely manner for individuals who do not currently hold a security clearance using the appropriate personnel security system.

Defense Logistics Agency Civilian Without a Security Clearance Was Not Reported in JPAS—Cardholder 2

A civilian from the Defense Logistics Agency (DLA) misused her travel card 32 times totaling \$5,500. During the prior audit we found that DLA took appropriate and timely action related to the travel card misuse. Specifically, DLA:

- immediately deactivated the cardholder’s travel card;
- suspended the cardholder for 3 days without pay; and
- removed the cardholder’s APC from travel card oversight responsibilities.

³⁸ Suitability determinations consider factors similar to security clearance determination, including misconduct or negligence in employment.

The prior audit did not review the security process related to the cardholder's misuse. The individual's JPAS records showed no incident reports related to travel card misuse. Therefore, no indication will exist of the travel card misuse and the associated disciplinary action if the individual is ever submitted for a suitability determination or for a security clearance adjudication.

DoD Management Did Not Help Cardholders With Possible Gambling Addictions or Financial Concerns in a Timely Manner

DoD commanders and supervisors missed opportunities to offer counseling for cardholders for possible gambling addictions or financial concerns. DoD Guidance³⁹ encourages the Heads of all DoD Components to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical, or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long-term, job-related security problems.

Two resources are available to assist in these areas of concern:

- **Military OneSource.** A confidential DoD-funded program for military personnel and military family members for a wide variety of assistance including stress, financial, reintegration, relationships, loss and grief, gambling, and many other areas.
- **Employee Assistance Program.** Serves DoD civilians and their families and covers similar areas described under Military OneSource.

The Director, DTMO should revise the "Government Travel Charge Card Regulations," March 2016 to require commanders or supervisors to consider whether available personnel assistance programs would be beneficial when travel card personal use, misuse, abuse, or fraud identify gambling or financial concerns.

³⁹ DoD 5200.02-R "Personnel Security Program," January 1987, as amended February 23, 1996.

Conclusion

DoD management did not perform reviews or performed inadequate reviews of cardholders when notified that cardholders potentially misused their travel card at casinos and adult entertainment establishments. In addition, DoD management took inconsistent actions on cardholders who misused their travel card. Cardholders received improper overpayments that directly reimbursed, indirectly may have reimbursed, or both the cardholder for personal use of the travel card. Finally, DoD management did not consistently consider the security implications of improper personal use of the travel card.

As a result, DoD management did not identify cardholders with prior misuse or eliminate further misuse of the travel card. DoD also missed opportunities to identify and recover inflated expenses on travel vouchers that directly reimbursed, indirectly may have reimbursed, or both cardholders for personal use of the travel card. In addition, DoD experienced potential national security vulnerabilities due to the lack of adjudication for cardholders with possible security concerns including, extensive travel card misuse, questionable judgment, the decision not to follow rules and guidance, financial concerns, or gambling addictions. Cardholders were not offered assistance through the employee assistance programs related to gambling addictions and financial concerns.

Management Comments on the Finding and Our Response

Deputy Assistant Secretary for Military Personnel Policy

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, noted the personal use identified in the report amounted to less than 0.04 percent of the total travel card spending and less than 0.03 percent of the total transaction volume. He stated the identified improper reimbursements were less than 0.001 percent of the total DoD travel payments. In addition, he maintained that more than half of improper reimbursements were attributable to a single cardholder. He also stated the report did not explain that not all the improper reimbursements were related to improper use of the travel card. Citing this information and delinquency rates of the travel card for DoD, the Deputy Assistant Secretary maintained the overall success of the program and the diligence of the agency program coordinators.

Our Response

The audit focused on three areas, including management actions taken for addressing travel card misuse, reviewing travel vouchers to identify improper payments, and considering security implications for travel card misuse. The scope of the audit included only those cardholders who were identified and provided to the APCs as part of Report No. DODIG-2015-125. Therefore, we cannot draw conclusions on the total amount of personal use in the travel card program, or the overall strength of the program. However, the Deputy Assistant Secretary's comments minimize the importance of our findings. We identified significant weaknesses in the oversight of the travel program as a result of our review of only 30 cardholders, and we also identified significant deficiencies in how DoD travel officials responded to our previous audit. The Deputy Assistant Secretary's comments, attempt to minimize the potential risks presented by our findings, including the risk of security vulnerabilities by cardholders who misused travel cards.

Recommendations, Management Comments, and Our Response

Recommendation 1

We recommend that the Under Secretary of Defense for Intelligence revise DoD 5200.2-R "Personnel Security Program," to require commanders or supervisors, in coordination with security personnel, to:

- a. Report incidents of travel card misuse under investigation or management review to the appropriate adjudicative facility in a timely manner using the appropriate personnel security system.**
- b. Report the outcome of the travel card misuse investigation including the results of the investigation and any administrative or disciplinary actions taken to the appropriate adjudicative facility using the appropriate personnel security system.**
- c. Report incidents of travel card personal use, misuse, abuse, or fraud under investigation or management review in a timely manner for individuals who do not currently hold a security clearance using the appropriate personnel security system.**

Under Secretary of Defense for Intelligence Comments

The Director, Counterintelligence and Security, Office of the Undersecretary of Defense for Intelligence, responding for the Under Secretary of Defense for Intelligence, agreed, stating that the Under Secretary of Defense for Intelligence will add the recommended requirements to DoD 5200.02-R. The Under Secretary also stated that the Regulation was converted to a manual and is expected to be published by December 31, 2016.

Our Response

Comments from the Director addressed the specifics of the recommendation, and no further comments are required.

Recommendation 2

We recommend the Director, Defense Travel Management Office:

- a. Improve the identification of personal use of the travel card and disciplinary actions taken by revising the “Government Travel Charge Card Regulations,” March 2016, to:**
 - 1. Require agency program coordinators to review the cardholder’s transaction history to identify any additional travel card personal use, misuse, abuse, or fraud after misuse is suspected or referred for review.**
 - 2. Require component program managers and agency program coordinators to verify the accurate employment status of a cardholder who has been identified or referred to DoD management for travel card personal use, misuse, abuse, or fraud.**
 - 3. Require commanders or supervisors to consider whether available personnel assistance programs would be beneficial when travel card personal use, misuse, abuse, or fraud identify gambling or financial concerns.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions the Defense Travel Management Office would take to accomplish the recommendations. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

b. Improve the actions taken to eliminate travel card misuse by cardholders with prior misuse by revising the “Government Travel Charge Card Regulations,” March 2016, to:

- 1. Require agency program coordinators to monitor the activity of cardholders with prior misuse and report any additional travel card personal use, misuse, abuse, or fraud to the commander or supervisor immediately.**
- 2. Require agency program coordinators, in conjunction with DoD management, and component program managers to consider reducing the credit limit and automated teller machine limit for cardholders with prior misuse.**
- 3. Require the losing activity to notify the gaining activity of detected travel card personal use, misuse, abuse, or fraud for any transferring cardholders.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions the Defense Travel Management Office would take to revise the “Government Travel Charge Card Regulations.” Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

- c. Establish a working group with Citibank, component program managers, and others necessary to identify whether automated tools exist or could be developed to deactivate and close the travel card account automatically when cardholders separate.**

Deputy Assistant Secretary for Military Personnel Policy

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed, stating that the Defense Travel Management Office has a quarterly meeting with Citibank and component program managers. The Defense Travel Management Office will explore the availability and feasibility of automated tools at those meetings.

Our Response

Comments from the Deputy Assistant Secretary addressed the specifics of the recommendation, and no further comments are required.

- d. Revise the Defense Travel Management Office “Travel Card – Agency Program Coordinator” course to:**
- 1. Include examples of the types of travel card personal use, misuse, abuse, or fraud previously detected by DoD management.**
 - 2. Include detailed information on the steps agency program coordinators should take when travel card personal use, misuse, abuse, or fraud is found and who to contact including the commander or supervisor, travel office, comptroller office, security office, legal office, and human resources office.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions the Defense Travel Management Office would take to revise the Defense Travel Management Office “Travel Card – Agency Program Coordinator” course. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

- e. Revise the Defense Travel Management Office “Travel Card 101” training course to include examples of the types of travel card personal use, misuse, abuse, or fraud previously detected by DoD management.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions that the Defense Travel Management Office would take to revise the Defense Travel Management Office “Travel Card 101” training course. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

- f. Develop a training course for DoD management on their responsibilities when potential travel card personal use, misuse, abuse, or fraud is detected to:**
- 1. Include detailed information on the steps DoD management should take and who to contact, including the commander or supervisor, APC, travel office, comptroller office, security office, legal office, and human resources office.**
 - 2. Include security reporting requirements.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions that the Defense Travel Management Office would take to develop a training course for DoD Management on the responsibilities when potential travel card personal use or misuse is detected. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

- g. Improve internal controls over the identification of travel overpayments by revising the “Government Travel Charge Card Regulations,” March 2016, to require DoD management and authorizing officials to:**
 - 1. Compare travel vouchers to travel card activity to ensure lodging and meals and incidental expenses charges are valid, accurate, and supported when travel card personal use, misuse, abuse, or fraud is identified or suspected.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions that the Defense Travel Management Office would take to improve internal controls over the identification of travel overpayments. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

- 2. Review travel card transactions incurred by cardholders outside of official travel locations and other relevant sources of cardholder location to identify inflated or false mileage claims when travel card personal use, misuse, abuse, or fraud is identified or suspected.**

Deputy Assistant Secretary for Military Personnel Policy

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed, stating that the Defense Travel Management Office will convene a working group with the Services to develop a definition of “outside of official travel locations” and a methodology to review actual travel card transactions.

Our Response

Comments from the Deputy Assistant Secretary addressed the specifics of the recommendation, and no further comments are required.

3. **Review mileage that is manually entered and not based on the Defense Table of Official Distances to identify inflated mileage when travel card personal use, misuse, abuse, or fraud is identified or suspected.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions that the Defense Travel Management Office would take to improve internal controls over the identification of travel overpayments. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

4. **Review local mileage to identify mileage that is not reimbursable, including mileage claims for travel to restaurants or to perform personal errands when travel card personal use, misuse, abuse, or fraud is identified or suspected.**

Deputy Assistant Secretary for Military Personnel Policy

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed, stating that the requirement would be more appropriate for inclusion in the Financial Management Regulations. The Deputy Assistant Secretary agreed to work with the Office of the Under Secretary of Defense (Comptroller) to determine the best resolution for this recommendation.

Our Response

Comments from the Deputy Assistant Secretary addressed the specifics of the recommendation, and no further comments are required.

- h. Revise the “Defense Travel System Regulations,” October 2015 to require travelers, authorizing officials, or non-defense travel system entry agents to amend travel vouchers within 5 days of identifying travel overpayments to establish a debt to recover the overpayment.**

Deputy Assistant Secretary for Military Personnel Policy

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed, stating that the Office of the Under Secretary of Defense (Comptroller) is currently drafting a directive-type memorandum to address the recommendation.

Our Response

Comments from the Deputy Assistant Secretary addressed the specifics of the recommendation, and no further comments are required.

- i. Address potential national security vulnerabilities by revising the “Government Travel Charge Card Regulations,” March 2016, to:**
 - 1. Report incidents of travel card personal use, misuse, abuse, or fraud under investigation or management review to the appropriate adjudicative facility in a timely manner using the appropriate personnel security system, and update with the final disciplinary action taken.**
 - 2. Include the commander’s and supervisor’s security reporting requirements for travel card personal use, misuse, abuse, or fraud.**

Management Comments Required

The Deputy Assistant Secretary for Military Personnel Policy, responding for the Director, Defense Travel Management Office, agreed but did not state what actions that the Defense Travel Management Office would take to address the potential national security vulnerabilities in the Travel Regulations. Therefore, we request comments to the final report that describe what specific actions the Defense Travel Management Office has taken or plans to take, and include the actual or planned completion dates of the actions.

Appendix A

Scope and Methodology

We conducted this performance audit from September 2015 through June 2016 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

On May 27, 2015, the Senate Committee on Armed Services requested this audit as a follow-on review of the transactions identified in Report No. DODIG-2015-125.

We designed the audit to answer the request by accomplishing the following objectives.

- Determine the extent to which cardholders misused their travel card, including personal use at casinos and adult entertainment establishments, and identify management actions taken as a result of the misuse.
- Identify whether cardholders sought or received improper overpayments from travel reimbursements.
- Determine whether cardholder management considered security implications and reported cardholders who misused their travel card.
- Assess whether any applicable labor agreements prevented cardholder management from taking action against cardholders for travel card misuse.

We nonstatistically selected a sample of 30 cardholders with the highest dollar amount of high-risk transactions at casinos, adult entertainment establishments, or both from the data obtained during the prior audit, which included 4,437 casino transactions totaling \$952,258 and 900 adult entertainment transactions totaling \$96,576. To select the sample, we included:

- the 7 cardholder examples from the prior audit report;
- the 4 cardholders with transaction activity exceeding \$1,000 at adult entertainment establishments; and
- the top 19 cardholders based on total dollar value of ATM and quasi cash activity at casinos.

For each cardholder in our sample, we performed steps to meet the audit objectives described above. We also met with personnel from each cardholder's command. Generally, these meetings were attended by the:

- commander or supervisor (referred to as DoD management);
- component program manager;
- agency program coordinator;
- authorizing official;
- lead defense travel administrator;
- comptroller office;
- security office; and
- human resource office.

In preparation for these meetings, we referred additional personal use transactions identified during the current audit and potential improper overpayments based on our review of travel vouchers. During the meetings, we also discussed management actions, security considerations, and labor agreement impacts.

Travel Card Personal Use and Management Actions

We obtained a list of all travel card transactions that occurred from October 2010 through June 2015⁴⁰ for each cardholder from the CitiBank Custom Reporting Service. We reviewed the transaction activity for potential personal use at casinos and adult entertainment establishments, including the transactions referred to management during the prior audit. We also compared the travel card transaction activity to the travel voucher documentation included in the scope of the audit to identify personal use transactions that occurred outside of official travel periods, where applicable. Lastly, we reviewed the travel card transactions for rejected cardholder payments due to insufficient funds, late payment charges and any other indications of account delinquency.

Through meetings with each cardholder's management, we determined the management actions taken against the cardholders based on the transactions referred during the prior audit. We also referred any newly identified personal use transactions based on the current scope and determined whether management intended to take additional action against cardholders who continued to misuse their travel card. Finally, we performed necessary follow up with cardholder management to confirm the status of any additional actions taken resulting from this audit.

⁴⁰ We expanded the scope of our travel card transaction review for some cardholders, as needed on a case-by-case basis.

We also reviewed the following criteria related to management of the travel card program and travel card misuse.

- Public Law 112-194, “Government Charge Card Abuse Prevention Act of 2012,” October 5, 2015
- DoD 7000.14-R, “Financial Management Regulation,” Volume 9, Chapter 3, “Department of Defense Government Travel Charge Card (GTCC),” April 2014
- DoD Instruction 5154.31, Volume 4, “Department of Defense Government Travel Charge Card Regulations,” October 2015
- DTMO “Government Travel Charge Card Regulations,” March 2016

Travel Voucher Improper Payments

We obtained travel vouchers for each cardholder for all official travel occurring from July 2013 through June 2015, including travel vouchers from the DTS, Reserve Travel System (RTS), and Corps of Engineers Financial Management System (CEFMS). We reviewed the vouchers for potential overpayments that either directly reimbursed, indirectly may have reimbursed, or both the cardholders for travel card misuse. Specifically, we identified reimbursements directly related to travel card misuse such as ATM fees associated with personal use at casinos or adult entertainment establishments and travel expenses associated with rental car travel to casinos located outside of official TDY locations. We also identified overpayments that may have indirectly reimbursed cardholders for misuse such as compensation for travel that did not occur, inflated ATM fees, inflated M&IE, and payments for lodging when the casino provided the room free of charge.

We provided the identified potential overpayments to cardholder management for further review. We performed necessary follow-up to determine whether management confirmed that the potential overpayments were improper overpayments, and whether management amended the corresponding travel vouchers to initiate collection. Lastly, we identified the amount of overpayments collected.

We reviewed the criteria listed below as it related to improper payments and reimbursable travel expenses.

- Public Law 107-300 “Improper Payments Information Act of 2002,” November 26, 2002
- Public Law 111-204 “Improper Payments Elimination and Recovery Act of 2010,” July 22, 2010

- Public Law 112-248 “Improper Payments Elimination and Recovery Improvement Act of 2012,” January 10, 2013
- OMB Circular No. A-123, Appendix C, “Requirements for Effective Estimation and Remediation of Improper Payments,” October 20, 2014
- The Joint Travel Regulations, “Uniformed Service Members and DoD Civilian Employees”⁴¹
- DoD Financial Management Regulations Volume 9, Chapter 2: “Defense Travel System (DTS)”
- DTMO “Defense Travel System Regulations,” October 2015

Security Clearance Considerations

We obtained JPAS records for each sample cardholder periodically throughout the audit to identify their security clearance. We also reviewed the JPAS records to determine whether management reported any incidents related to the cardholders’ travel card misuse. We confirmed the accuracy of the JPAS information during meetings held with cardholder management.

We met with personnel at the DoD Consolidated Adjudications Facility to determine its roles and responsibilities related to security clearance determinations, including specific policies governing such determinations and systems used. We also met with personnel from the DoD Consolidated Adjudications Facility, as well as personnel from the Defense Intelligence Agency Central Adjudication Facility, to determine the specific adjudication factors considered for seven sample cardholders.

Additionally, we reviewed the following criteria pertaining to personnel security policies and travel card misuse.

- DoD Instruction 5154.31, Volume 4, “Department of Defense Government Travel Charge Card Regulations,” October 2015
- DoD Instruction 5200.02, “DoD Personnel Security Program (PSP),” September 9, 2014
- DoD 5200.2-R, “Department of Defense Personnel Security Program,” January 1987, amended February 23, 1996
- OPM memorandum “Introduction of Credentialing, Suitability, and Security Clearance Decision-Making Guide,” January 14, 2008

⁴¹ The JTR is published monthly. We reviewed each version applicable to the scope of our travel voucher review.

Labor Agreement Impact

During meetings with each sample cardholder's management, we determined whether the cardholder was employed under a labor agreement. For cardholders employed under a labor agreement, we inquired whether management determined the applicable labor agreement restricted them from taking action against cardholders who misused their travel card. We also obtained copies of the labor agreements and reviewed any sections related to disciplinary actions to confirm management's interpretation regarding their ability to take action in instances of travel card personal use.

Use of Computer-Processed Data

The data we obtained during the audit were sufficiently reliable for the purposes of our audit. We used computer-processed data from the following systems.

Visa IntelliLink Compliance Management

We used Visa's IntelliLink Compliance Management system to access its transactional data and develop our sample cardholder list. Visa has extensive security standards that require all entities that store, process, or transmit Visa cardholder data—including financial institutions, merchants and service providers—to comply with an industry standard known as the Payment Card Industry (PCI) Data Security Standard. The PCI Security Standards Council oversees the security standards that include a compliance program for:

- assessing controls;
- reporting or validating controls, or both, are in place; and
- monitoring or alerting, or both, of existing controls.

The PCI Data Security Standard certification for Visa IntelliLink Compliance Management was valid through December 31, 2016. Therefore, we determined the Visa data were sufficiently reliable.

Citi Electronic Access Systems

We obtained travel card data from the Citi Electronic Access Systems at Citibank to identify personal use by the 30 cardholders in our sample. We obtained reasonable assurance through an independent service auditor review of Citibank's technology infrastructure in Service Organization Control reports. The reports asserted the controls were suitably designed to operate effectively and provided reasonable assurance that the control objectives were achieved and operated effectively, therefore we concluded the data were sufficiently reliable.

DTS

We used DTS to obtain travel voucher data to identify overpayments. In 2013, DLA completed a readiness review of DTS system controls and subsequently asserted on December 11, 2013, that the DTS information technology system control activities were ready for audit. On September 25, 2015, the DLA OIG issued the results of the audit, "Statement of Standards for Attestation Engagement No. 16 SSAE 16." The SSAE 16 audit provided reasonable assurance of the input, processing, or output of DTS data, so we concluded the data were sufficiently reliable.

RTS

The Reserve Travel System computes and reimburses travelers performing travel within Air Force Reserve Command. We used RTS travel voucher data to identify overpayments for one cardholder. As part of a 2014 Air Force Audit Agency report, the auditors recommended strengthening RTS controls to enhance data integrity and provide more accurate, complete, and reliable data. However, the report also indicated that the auditors conducted testing on RTS lodging and M&IE expenses and determined they were correctly calculated. We compared the vouchers to receipts provided and did not identify any problems for the vouchers reviewed. Therefore, we concluded the data were sufficiently reliable.

CEFMS

We used CEFMS travel voucher data to identify overpayments for one Army Corps of Engineers cardholder. According to the FY 2015 Army Annual Financial Report, CEFMS is the principal financial management system used by Army Corps of Engineers for all financial transactions. During the 2015 Army Corps of Engineers audit, an independent audit agency performed control testing on CEFMS. Two of the controls tested were related to travel vouchers and both were determined to be effective for design, implementation, and effectiveness. We also compared the vouchers to receipts provided and did not identify any problems for the vouchers reviewed. Therefore, we concluded the data were sufficiently reliable.

JPAS

We used JPAS data to identify the clearance eligibility and security incident history for the selected cardholders. According to a Defense Manpower Data Center official, neither an internal stakeholder nor a third-party organization has reviewed the internal controls of JPAS. To obtain reasonable assurance, we verified the cardholders' security clearance eligibility and if an incident was reported during the meetings with DoD management. We did not identify concerns that would impact our audit and determined the data were sufficiently reliable.

Use of Technical Assistance

We met with the Quantitative Methods Division during the planning phase of the audit and discussed the proposed scope and sample size for the cardholder reviews. In addition, we met with the DoD IG Office of Security to determine how travel card misuse affects security clearances and obtain JPAS records for the sample cardholders.

Prior Coverage

During the last 5 years, the Department of Defense Inspector General (DoD IG) issued one report discussing travel card misuse. Unrestricted DoD IG reports can be accessed at <http://www.dodig.mil/pubs/index.cfm>.

DoD IG

Report No. DODIG-2015-125, “DoD Cardholders Used Their Government Travel Cards for Personal Use at Casinos and Adult Entertainment Establishments,”
May 19, 2015

Appendix B

Senate Committee on Armed Services Request

JOHN MCCAIN, ARIZONA, CHAIRMAN
 JAMES M. INHOFE, OKLAHOMA
 JEFF SESSIONS, ALABAMA
 ROGER F. WICKER, MISSISSIPPI
 KELLY AYOTTE, NEW HAMPSHIRE
 DEB FISCHER, NEBRASKA
 TOM COTTON, ARKANSAS
 MIKE ROUNDS, SOUTH DAKOTA
 JONI ERNST, IOWA
 THOM TELLIS, NORTH CAROLINA
 DAN SULLIVAN, ALASKA
 MIKE LEE, UTAH
 LINDSEY GRAHAM, SOUTH CAROLINA
 TED CRUZ, TEXAS

JACK REED, RHODE ISLAND
 BILL NELSON, FLORIDA
 CLAIRE MCCASKILL, MISSOURI
 JOE MANCHINI II, WEST VIRGINIA
 JEANNE SHAHEEN, NEW HAMPSHIRE
 KRISTEN E. GILLIBRAND, NEW YORK
 RICHARD BLUMENTHAL, CONNECTICUT
 JOE DONNELLY, INDIANA
 MAZIE HIRONO, HAWAII
 TIM KAINE, VIRGINIA
 ANDRUS S. KING, JR., MAINE
 MARTIN HEINRICH, NEW MEXICO

United States Senate
 COMMITTEE ON ARMED SERVICES
 WASHINGTON, DC 20510-6050

CHRISTIAN D. BROSE, STAFF DIRECTOR
 ELIZABETH L. KING, MINORITY STAFF DIRECTOR

May 27, 2015

The Honorable Jon T. Rymer
 Inspector General
 Department of Defense
 4800 Mark Center Drive
 Alexandria, Virginia 22350-1500

Dear Inspector General Rymer:

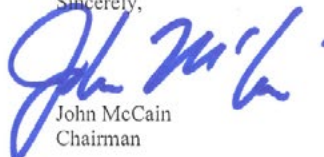
Thank you for your report titled "DoD Cardholders Used Their Government Travel Cards for Personal Use at Casinos and Adult Entertainment Establishments." You identified over 5,000 such transactions totaling more than \$1 million in the course of a single year. This finding is very troubling. While I recognize that this figure represents only a small fraction of travel card spending over the period, it is a violation of the Department's policies, and your report clearly indicates that internal controls are insufficient to identify and stop such activities. I am encouraged that you recommended the Department take steps to accomplish this.

At the same time, the improper personal use of travel cards raises additional risks for the Department that warrant further investigation. Your report does not indicate or confirm whether the Department has, in fact, provided reimbursement for the kinds of improper charges you have identified. While the Department has provided assurances that this is not the case, that assertion needs confirmation to ensure that taxpayer funds, regardless of the amount, are not being so egregiously wasted. Furthermore, personal use of government travel cards to engage in gambling activities, aside from being improper, could pose additional risks if an employee holds a security clearance. As such, I am requesting that you conduct an additional review that addresses the following questions:

- To what extent did the cardholders who engaged in improper personal use of their travel charge cards seek and/or receive reimbursement for the improper charges, and if so what action is the Department pursuing in these cases?
- To what extent is the Department reconciling data on improper personal use of travel cards to identify cardholders who hold security clearances and consider whether it is appropriate to maintain those clearances?
- What labor agreements are in place that may restrict the Department's ability to take disciplinary action in cases where individuals engage in improper personal use of government travel charge cards?

If you have any questions regarding this inquiry, please contact [REDACTED] on my staff, at [REDACTED].

Sincerely,


 John McCain
 Chairman

Appendix C

Travel Card Misuse and Management Actions

Table 1. Summary of Travel Card Misuse and Management Actions Taken

Card-holder Number	Service/ Agency	Type of Transaction	Transactions Referred During Prior Audit	Total Dollar Amount of Referred Transactions- Prior Audit	Action Taken- Prior Audit	Additional Personal Use Transactions Identified ¹	Total Dollar Amount of Additional Transactions Identified	Additional Action Taken (After Meeting with Management)
1	Army	Casino	107	\$21,429.25	Issued a Letter of Reprimand	0	\$0	General Officers Memorandum of Reprimand
2	DLA	Casino	31	5,400.25	Deactivated travel card and suspended 3 days without pay	1	100.00	No additional action
3	Air Force	Casino	7	1,564.50	No action taken/ labor agreement	0	0	No additional action
4	Air Force	Adult	3	4,686.00	Reduction in rank, Unfavorable Information File Established, and GTCC Training	0	0	No additional action
5	Navy	Adult	2	2,100.00	Counseled	0	0	No additional action
6	Marine Corps	Adult	3	1,614.40	7-day suspension	0	0	No additional action
7	Navy	Both	18	1,606.19	Counseled, training, and statement of understanding	1	29.00	Reduction in rank (suspended) ²
8	Army	Casino	9	2,860.24	Counseled	39	10,476.25	General Officer Memorandum of Reprimand
9	Air Force	Casino	24	10,384.00	Reduction in rank (suspended) ²	39	11,058.00	No additional action ³

Footnotes used throughout this Appendix are defined on the final page.

Table 1. Summary of Travel Card Misuse and Management Actions Taken (cont'd)

Card-holder Number	Service/ Agency	Type of Transaction	Transactions Referred During Prior Audit	Total Dollar Amount of Referred Transactions- Prior Audit	Action Taken- Prior Audit	Additional Personal Use Transactions Identified ¹	Total Dollar Amount of Additional Transactions Identified	Additional Action Taken (After Meeting with Management)
10	Army	Adult	6	1,580.00	30-day suspension	6	1,020.00	No additional action
11	Navy	Adult	3	1,417.00	Counseled/ retrained/new statement of understanding/ PG-13	0	0	No additional action
12	Air Force	Adult	2	1,101.00	Verbal counseling	0	0	No additional action
13	Navy	Adult	1	1,078.00	Nonpunitive letter of caution	0	0	No additional action
14	Air Force	Casino	23	4,151.59	Verbal counseling, training, and statement of understanding	66	10,219.33	Letter of Counseling
15	Air Force	Casino	13	3,852.00	Letter of Reprimand and travel card deactivated	85	8,046.30	No additional action
16	Army	Casino	11	3,798.98	Developmental counseling form	15	3,088.50	General Officer Memorandum of Reprimand & Letter of Concern for civilian position
17	Air Force/ USSOCOM ⁴	Casino	8	3,634.96	No action taken	44	9,271.02	Letter of Counseling and training
18	Navy	Casino	12	2,822.97	Counseled	61	14,150.95	2-week suspension
19	Air Force	Casino	8 ⁵	2,726.92	7 day suspension, directed financial counseling, and Letter of Reprimand ⁶	353	29,812.51	No additional action

Footnotes used throughout this Appendix are defined on the final page.

Table 1. Summary of Travel Card Misuse and Management Actions Taken (cont'd)

Card-holder Number	Service/ Agency	Type of Transaction	Transactions Referred During Prior Audit	Total Dollar Amount of Referred Transactions- Prior Audit	Action Taken- Prior Audit	Additional Personal Use Transactions Identified ¹	Total Dollar Amount of Additional Transactions Identified	Additional Action Taken (After Meeting with Management)
20	DTRA	Casino	5	2,522.50	Letter of Reprimand from DTRA and advisory letter from the DICAf	19 ⁷	6,960.50	Pending Legal Review of Investigation
21	Army	Casino	18	2,476.96	Member retired/ no action taken	7	1,229.96	None because cardholder was retired
22	Navy	Casino	16	2,438.75	None/not considered personal use	258	29,292.75	Counseled, revoked access to classified information, administrative leave, retired
23	Air Force	Casino	6	2,430.70	Counseling, Letter of Reprimand, and Deactivated GTCC	21	7,552.22	No additional action
24	Army	Casino	14	2,263.00	Member retired/ no action taken	84	10,968.86	None because cardholder was retired
25	Army	Casino	10	2,241.99	APC did not inform Command/no action taken	27	5,518.83	Investigation complete, Due-process in progress
26	Air Force	Casino	7	2,188.49	6-month suspension ⁸	3	971.25	Clearance suspended and member placed on terminal leave (no additional action due to cardholder retiring)

Footnotes used throughout this Appendix are defined on the final page.

Table 1. Summary of Travel Card Misuse and Management Actions Taken (cont'd)

Card-holder Number	Service/ Agency	Type of Transaction	Transactions Referred During Prior Audit	Total Dollar Amount of Referred Transactions- Prior Audit	Action Taken- Prior Audit	Additional Personal Use Transactions Identified ¹	Total Dollar Amount of Additional Transactions Identified	Additional Action Taken (After Meeting with Management)
27	Army Corps of Engineers	Casino	9	2,169.00	None/not considered personal use	11	2,158.00	Counseled, retrained, and warned that reoccurrence would result in terminated employment
28	Army	Casino	14	2,013.50	Command was not aware/no action taken	18	2,387.96	Letter of Reprimand
29	Army	Casino	5	1,925.99	Verbal counseling	4	692.00	No additional action
30	Army/ Navy/ OUSD ⁹	Casino	9	1,836.00	Member left command/no action taken	8	1,726.70	Counseled by supervisor and training
Total			404	\$102,315.13		1,170	\$166,730.89	

¹ The number of transactions in this column include the number of casino and/or adult entertainment transactions we identified, as well as any personal use transactions we identified that were outside of official travel (see Appendix A).

² The disciplinary action was suspended for 6 months. This means that as long as the cardholder did not violate the Uniform Code of Military Justice within that time period, there would be no loss in rank or other disciplinary action, and the misuse would not be recorded in his personnel file.

³ Initial action taken by command in Prior Audit column was based on full review which included the additional personal use transactions we identified for this audit. Therefore, there was no additional management action was taken.

⁴ Cardholder is a member of the Air Force currently working for and disciplined by US Special Operations Command (USSOCOM).

⁵ Includes only the referred ATM casino withdrawals. We referred an additional 10 transactions for \$2,792.24.

⁶ The letter of reprimand occurred in October 2011, before our prior audit.

⁷ We reviewed additional transactions outside the scope of our audit for this cardholder (See Appendix A). Therefore, this number includes two transactions that occurred after June 2015.

⁸ The cardholder continued to work. If there were no new incidents during the next 6 months, the suspension would be lifted.

⁹ The cardholder was a naval reservist detailed to a joint entity administratively supported by the Army at the time of the misuse. Actions were taken by the Office of the Under Secretary of Defense (Intelligence) (OUSD(I)), where he is currently detailed.

Appendix D

Travel Overpayments

Table 2. Summary of Travel Overpayments

Cardholder Number	Service/Agency	Number of Vouchers Reviewed	Number of Vouchers with Overpayments	Total Dollar Amount of Overpayments Identified ¹	Total Dollar Amount of AO Amendments to Voucher ²	Total Dollar Amount of Overpayments Collected	Number of Days from Meeting Until Voucher Amended	Number of Days From Meeting Until Debt Satisfied
1	Army	47	9	\$751.69	\$1,739.39 ³	\$0 ⁴	257	Debt not satisfied
2	DLA	0	0	0	N/A	N/A	N/A	N/A
3	Air Force	1	1	115.82	58.94	58.94	15	267
4	Air Force	2	0	0	N/A	N/A	N/A	N/A
5	Navy	3	0	0	N/A	N/A	N/A	N/A
6	Marine Corps	1	1	20.00	20.00	0 ³	204	Debt not satisfied
7	Navy	9	1	4.53	N/A	N/A	N/A	N/A
8	Army	17	10	325.65	326.33	205.07 ⁵	60	73
9	Air Force	4	0	0	N/A	N/A	N/A	N/A
10	Army	2	1	7.63	N/A	N/A	N/A	N/A
11	Navy	7	2	203.59	256.59	249.00 ⁶	15	24
12	Air Force	12	1	3.99	N/A	N/A	N/A	N/A
13	Navy	12	0	0	N/A	N/A	N/A	N/A
14	Air Force	20	9	238.45	26.87	0 ³	62	Debt not satisfied

Footnotes used throughout this Appendix are defined on the final page.

Table 2. Summary of Travel Overpayments (cont'd)

Cardholder Number	Service/Agency	Number of Vouchers Reviewed	Number of Vouchers with Overpayments	Total Dollar Amount of Overpayments Identified ¹	Total Dollar Amount of AO Amendments to Voucher ²	Total Dollar Amount of Overpayments Collected	Number of Days from Meeting Until Voucher Amended	Number of Days From Meeting Until Debt Satisfied
15	Air Force	7	1	14.00	14.00	14.00	131	147
16	Army	19	4	85.26	85.62	85.62	167	176
17	Air Force/ USSOCOM	13	7	633.76	650.81 ⁷	617.61 ⁸	27	176
18	Navy	41	8	64.90 ⁹	N/A	N/A	N/A	N/A
19	Air Force	1	1	0.17	N/A	N/A	N/A	N/A
20	DTRA	14	5	128.12	Pending Legal Review of Investigation	0	Pending Legal Review of Investigation	Pending Legal Review of Investigation
21	Army	17	13	302.91	302.91 ¹⁰	0	28	Debt not satisfied
22	Navy	36	31	4,890.58	No Adjustments as of August 8, 2016	0	N/A	Debt not satisfied
23	Air Force	6	2	75.81	60.00	60.00	116	132
24	Army	21	19	382.61	440.05 ¹¹	440.05	No Amendment ¹²	99
25	Army	32	2	267.00	473.75	0 ¹³	59	Debt not satisfied
26	Air Force	4	2	26.29	510.85	510.85	7	149
27	Army Corps of Engineers	10	0	0	N/A	N/A	N/A	N/A

Footnotes used throughout this Appendix are defined on the final page.

Table 2. Summary of Travel Overpayments (cont'd)

Cardholder Number	Service/Agency	Number of Vouchers Reviewed	Number of Vouchers with Overpayments	Total Dollar Amount of Overpayments Identified ¹	Total Dollar Amount of AO Amendments to Voucher ²	Total Dollar Amount of Overpayments Collected	Number of Days from Meeting Until Voucher Amended	Number of Days From Meeting Until Debt Satisfied
28	Army	15	0	0	N/A	N/A	N/A	N/A
29	Army	4	0	0	N/A	N/A	N/A	N/A
30	Army/Navy/ OUSDI	9	1	0.91	N/A	N/A	N/A	N/A
Total		386	131	\$8,543.67	\$4,966.11	\$2,241.14		

¹ According to DoD Regulations, dollar amounts under \$10 are not required to be collected. Therefore, if the total dollar amount of overpayments was less than \$10, the money will not be collected and the remaining columns in this spreadsheet will be N/A.

² This information in this column may be higher or lower than the amount identified by the audit team because cardholder management had additional information during their review that was not available to the audit team.

³ Additional travel vouchers have been referred for investigation to identify any additional overpayments.

⁴ DTS voucher was amended, due process served, and awaiting collection.

⁵ DTS has been amended, but one voucher in the amount of \$121.26 has not been collected. The debt is awaiting collection through payroll deduction.

⁶ \$7.59 of the total debt will not be collected because the voucher DUE US is less than \$10.

⁷ \$11.70 of this amount will not be collected because it applied to two vouchers and the amount per voucher was less than \$10.

⁸ The DTS vouchers were all amended; however one voucher for \$21.50 is still awaiting collection.

⁹ The aggregate total is over \$10; however, the total dollar amount per voucher was less than \$10, and will not be collected.

¹⁰ Submitted to DFAS Out-of-Service Debts.

¹¹ Certified Letter was sent to member requesting payment.

¹² Certified letter was sent to the cardholder because she was out of service and the amount was collected as a lump sum payment.

¹³ DTS voucher amended and collection through salary offset requested.

Appendix E

Security Clearance Considerations

Table 3. Summary of Security Clearance Considerations

Cardholder #	Service/ Agency	Security Clearance Eligibility	Management Coordinated with Local Security Based on Prior Audit	Local Security Office Reported Incident in JPAS (Prior to Meeting with Audit Team)	Local Security Office Reported Incident in JPAS After Meeting
1	Army	Top Secret	No	No	Yes
2	DLA	None	Yes	No	No
3	Air Force	None	No	No	No
4	Air Force	Top Secret	No	No	Yes
5	Navy	Top Secret	No	No	Yes
6	Marine Corps	None	No	No	No
7	Navy	Top Secret	Yes	No	Yes
8	Army	Top Secret	No	No	Yes
9	Air Force	Secret	Yes	No	No
10	Army	None	No	No	No
11	Navy	Top Secret	No	No	No
12	Air Force	Secret (CNWDI)*	No	No	No
13	Navy	Top Secret	No	No	No
14	Air Force	Secret	No	No	No
15	Air Force	Secret	No	No	No
16	Army	Secret	No	No	Yes
17	Air Force/ USSOCOM	Top Secret	No	No	No
18	Navy	Top Secret (CNWDI*)	Yes	No	Yes
19	Air Force	Secret	Yes	Yes	No
20	DTRA	Top Secret (CNWDI*)	Yes	Yes	Yes
21	Army	Secret	No	No	No
22	Navy	Secret	No	No	Yes
23	Air Force	Top Secret	No	No	No

Footnotes used throughout this Appendix are defined on the final page.

Table 3. Summary of Security Clearance Considerations (cont'd)

Cardholder #	Service/ Agency	Security Clearance Eligibility	Management Coordinated with Local Security Based on Prior Audit	Local Security Office Reported Incident in JPAS (Prior to Meeting with Audit Team)	Local Security Office Reported Incident in JPAS After Meeting
24	Army	Secret	No	No	No
25	Army	Secret	No	No	Yes
26	Air Force	Secret	Yes	No	Yes
27	Army Corps of Engineers	None	No	No	No
28	Army	Top Secret	No	No	No
29	Army	Secret	No	No	No
30	Army/Navy/ OUSDI	Top Secret	No	No	No

* The cardholder had DoD Critical Nuclear Weapon Design Information (CNWDI) Access. CNWDI is a DoD category of Top Secret Restricted Data or Secret Restricted Data that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device.

Management Comments

Office of the Under Secretary of Defense for Intelligence



INTELLIGENCE

OFFICE OF THE UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

29 JUL 2016

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel
Card Misuse at Casinos and Adult Entertainment Establishments (Project No.
D2015-D000CL-0221.000)

Thank you for the opportunity to review the draft report same subject. We found no
factual errors in the draft report and concur with the recommendation assigned to the Under
Secretary of Defense for Intelligence (USD(I)) for action.

USD(I) has updated the DoD 5200.02-R "Personnel Security Program," and converted it
to a manual. The manual is undergoing Legal Sufficiency Review and the recommended
reporting requirement identified in the report will be added. We expect to publish the manual by
December 31, 2016. The point of contact is [REDACTED]

for Carrie A. Wibben
Director, Counterintelligence and Security



Deputy Assistant Secretary for Military Personnel Policy



MANPOWER AND
RESERVE AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
1500 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-1500

AUG 5 2016

██████████
Program Director
Contract Management and Payments
Office of the Inspector General
Department of Defense
4800 Mark Center Drive
Alexandria, VA 22350

Dear ██████████

This letter responds to your request for Department of Defense (DoD) comments on the Office of the Inspector General draft report, "DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card Misuse at Casinos and Adult Entertainment Establishments," dated June 29, 2016 (Project No. D2015-D000CL-0221.000). Comments on the recommendations contained in the report are enclosed.

Although we concur with the recommendations, I believe it is important to note that the monetary amount of the personal use of the Government Travel Charge Card identified in the audit amounted to less than 0.04 percent of the total travel card spend and less than 0.03 percent of total transaction volume for the period covered by the audit. Most importantly, the \$8,500 identified in the report as improperly reimbursed amounts to less than 0.001 percent of the total DoD travel spend, which averages approximately \$8 billion per year.

While the report shows that approximately \$8,500 was improperly reimbursed, it does not explain that not all this amount was specifically related to improper use of the travel card itself, but that a portion was the result of improper travel payments discovered during the audit. Additionally, more than half of this amount (\$4,890.58) was attributable to a single cardholder.

Additionally, DoD delinquency rates for individually billed accounts averaged just over 1 percent. This compares to an industry average of over 4 percent, and is a strong indicator of the overall success of our program and the diligence of our agency program coordinators.

I appreciate the opportunity to comment on this report. My point of contact is ██████████ who can be reached at ██████████

Sincerely,

A. M. Kurta
Deputy Assistant Secretary
(Military Personnel Policy)

Enclosure:
As stated

Deputy Assistant Secretary for Military Personnel Policy (cont'd)

Defense Travel Management Office Comments on DoDIG Draft Report
“DoD Officials Did Not Take Appropriate Action When Notified of Potential Travel Card
Misuse at Casinos and Adult Entertainment Establishments”, dated June 29, 2016
(Project No. D2015-D000CL-0221.000)

Recommendation 2a1: Improve the identification of personal use of the travel card and disciplinary actions taken by revising the “Government Travel Charge Card Regulations,” March 2016, to require agency program coordinators to review the cardholder’s transaction activity to identify any additional travel card personal use, misuse, abuse, or fraud after misuse is suspected or referred for review.

Response: Concur.

Recommendation 2a2: Improve the identification of personal use of the travel card and disciplinary actions taken by revising the “Government Travel Charge Card Regulations,” March 2016, to require component program managers and agency program coordinators to verify the accurate employment status of a cardholder who has been identified or referred to DoD management for travel card personal use, misuse, abuse, or fraud.

Response: Concur.

Recommendation 2a3: Improve the identification of personal use of the travel card and disciplinary actions taken by revising the “Government Travel Charge Card Regulations,” March 2016, to require commanders or supervisors to consider whether available personnel assistance programs would be beneficial when travel card personal misuse, abuse, or fraud identifying gambling or financial concerns.

Response: Concur.

Recommendation 2b1: Improve the actions taken to eliminate travel card misuse by cardholders with prior misuse by revising the “Government Travel Charge Card Regulations,” March 2016, to require agency program coordinators to monitor the activity of cardholders with prior misuse and report any additional travel card personal use, misuse, abuse, or fraud to the commander or supervisor immediately.

Response: Concur.

Recommendation 2b2: Improve the actions taken to eliminate travel card misuse by cardholders with prior misuse by revising the “Government Travel Charge Card Regulations,” March 2016, to require agency program coordinators, in conjunction with DoD management, and component program coordinators to consider reducing the credit limit and automated teller machine limit for cardholders with prior misuse.

Response: Concur.

Deputy Assistant Secretary for Military Personnel Policy (cont'd)

Recommendation 2b3: Improve the actions taken to eliminate travel card misuse by cardholders with prior misuse by revising the "Government Travel Charge Card Regulations," March 2016, to require the losing activity to notify the gaining activity of detected travel card personal use, misuse, or fraud for any transferring cardholders.

Response: Concur.

Recommendation 2c: Establish a working group with Citibank, component program managers, and others necessary to identify whether automated tools exist or could be developed to deactivate and close the travel card account automatically when cardholders separate.

Response: The Defense Travel Management Office (DTMO) has a standing quarterly meeting with Citibank and component program managers. We will continue to explore with Citi the availability and feasibility of automated tools, like those discussed in this recommendation.

Recommendation 2d1: Revise the Defense Travel Management Office "Travel Card – Agency Program Coordinator" course to include examples of the types of travel card personal use, misuse, abuse, or fraud previously detected by DoD management.

Response: Concur.

Recommendation 2d2: Revise the Defense Travel Management Office "Travel Card – Agency Program Coordinator" course to include detailed information on the steps agency program coordinators should take when travel card personal use, misuse, or fraud is found and who to contact including the commander or supervisor, travel office, comptroller office, security office, legal office, and human resources office.

Response: Concur.

Recommendation 2e: Revise the Defense Travel Management Office "Travel Card 101" training course to include examples of the types of travel card personal use, misuse, abuse, or fraud previously detected by DoD management.

Response: Concur.

Recommendation 2f1: Develop a training course for DoD management on their responsibilities when potential travel card personal use, misuse, abuse, or fraud is detected to include detailed information on the steps DoD management should take and who to contact, including the commander or supervisor, APC, travel office, comptroller office, security office, legal office, and human resources office.

Response: Concur.

Recommendation 2f2: Develop a training course for DoD management on their responsibilities when potential travel card personal use, misuse, abuse, or fraud is detected to include security reporting requirements.

Deputy Assistant Secretary for Military Personnel Policy (cont'd)

Response: Concur.

Recommendation 2g1: Improve internal controls over the identification of travel overpayments by revising the "Government Travel Charge Card Regulations," March 2016, to require DoD management officials to compare travel vouchers to travel card activity to ensure lodging and meals and incidental expenses charged are valid, accurate, and supported when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Response: Concur.

Recommendation 2g2: Improve internal controls over the identification of travel overpayments by revising the "Government Travel Charge Card Regulations," March 2016, to require DoD management officials to review travel card transactions incurred by cardholders outside of official travel locations and other relevant sources of cardholder location to identify inflated or false mileage claims when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Response: Concur in concept. DTMO will convene a working group with the Services to develop a definition of "outside of official travel locations" and a methodology to review actual travel card transactions; that capability is not currently resident in DTS.

Recommendation 2g3: Improve internal controls over the identification of travel overpayments by revising the "Government Travel Charge Card Regulations," March 2016, to require DoD management officials to review mileage that is manually entered and not based on the Defense Table of Official Distances to identify inflated mileage when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Response: Concur

Recommendation 2g4: Improve internal controls over the identification of travel overpayments by revising the "Government Travel Charge Card Regulations," March 2016, to require DoD management officials to review local mileage to identify mileage that is not reimbursable, including mileage claims for travel to restaurants or to perform personal errands when travel card personal use, misuse, abuse, or fraud is identified or suspected.

Response: We believe the requirements discussed in this recommendation would be more appropriate for inclusion in the Financial Management Regulations, which provide direction and guidance to travel voucher approving officials. We will work with the OSD Comptroller to determine the best resolution for this recommendation.

Recommendation 2h: Revise the "Defense Travel System Regulations," October 2015, to require travelers, authorizing officials, or non-defense travel systems entry agents to amend travel vouchers within 5 days of identifying travel overpayments to establish a debt to recover the overpayment.

Deputy Assistant Secretary for Military Personnel Policy (cont'd)

Response: Concur. The OSD Comptroller is currently staffing a Directive-Type Memorandum on this subject.

Recommendation 2i1: Address potential national security vulnerabilities by revising the "Government Travel Charge Card Regulations," March 2016, to report incidents of travel card personal use, misuse, abuse, or fraud under investigation or management review to the appropriate adjudicative facility in a timely manner using the appropriate personnel security system, and update with the final disciplinary action taken.

Response: Concur

Recommendation 2i2: Address potential national security vulnerabilities by revising the "Government Travel Charge Card Regulations", March 2016, to include the commander's and supervisor's security reporting requirements for travel card personal use, misuse, abuse, or fraud.

Response: Concur

Glossary

Agency Program Coordinators. APCs are DoD personnel (military or civilian), contractor, or foreign national employees who are designated in writing by a commander or director as responsible for managing the day-to-day operations of the travel card program.

Authorizing Official. Authorizing officials are responsible for reviewing and approving cardholder's travel vouchers.

Component Program Managers. CPMs are DoD personnel (military or civilian) designated in writing by the Component Head or designee responsible for establishing, managing and delegating responsibilities for their travel card program. The CPM is responsible for the overall management of the travel card program at a high level such as a Military Department or large Defense Agency.

The CPMs conduct periodic hierarchy level reviews, to include validating hierarchy level structure and verifying point of contact information. This process may be delegated down to lower levels. The CPMs ensure that travel cards are properly approved; reasonable credit limits are established and maintained; and annual reviews are performed to monitor credit limits and card utilization.

DoD Component Heads/Defense Agency Directors. The heads of the DoD Components are responsible for implementing Travel and Transportation Reform Act of 1998 for use in their Component. The Component Heads will also ensure all personnel, to include APCs, centrally billed account managers, and cardholders, are properly trained on travel card use and policy.

DoD Management. DoD management is the cardholders' commander or supervisor, or both. DoD management is responsible for ensuring that periodic internal control reviews are conducted for their travel card program. Those controls should ensure that:

- travelers submit travel vouchers within five days of completion of official travel and comply with split disbursement requirements;
- credit limits are adjusted/appropriate to meet mission requirements; and
- unused accounts are closed.

Findings of significant weaknesses should be reported to the CPM in addition to the command or agency head.

Human Resources Office. Human resources offices maintain the cardholder's personnel file.

Legal Office. A primary responsibility for legal offices is to advise command on investigations and disciplinary actions.

Office of Personnel Management. Updates security questionnaires (SF 86).

Security Office. Security offices are the activities liaison between the command and the adjudicative facilities.

Acronyms and Abbreviations

APC	Agency Program Coordinator
ATM	Automated Teller Machine
CEFMS	Corps of Engineers Financial Management System
CPM	Component Program Manager
DICAF	Defense Intelligence Central Adjudication Facility
DLA	Defense Logistics Agency
DMDC	Defense Manpower Data Center
DTMO	Defense Travel Management Office
DoD FMR	Department of Defense Financial Management Regulation
DTRA	Defense Threat Reduction Agency
DTS	Defense Travel System
JPAS	Joint Personnel Adjudication System
JTR	Joint Travel Regulations
M&IE	Meals and Incidental Expenses
OMB	Office of Management and Budget
OUSD	Office of the Under Secretary of Defense
PCI	Purchase Card Industry
RTS	Reserve Travel System
SF 86	Standard Form 86
TDY	Temporary Duty



Whistleblower Protection

U.S. DEPARTMENT OF DEFENSE

The Whistleblower Protection Ombudsman's role is to educate agency employees about prohibitions on retaliation and employees' rights and remedies available for reprisal. The DoD Hotline Director is the designated ombudsman. For more information, please visit the Whistleblower webpage at www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison

congressional@dodig.mil; 703.604.8324

Media Contact

public.affairs@dodig.mil; 703.604.8324

For Report Notifications

www.dodig.mil/pubs/email_update.cfm

Twitter

www.twitter.com/DoD_IG

DoD Hotline

www.dodig.mil/hotline



DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098

